

# **EXHIBIT 78**

## **4/15/22 EXPERT REPORT OF PROF. ON AMIR**

*CONFIDENTIAL*  
*SUBJECT TO PROTECTIVE ORDER*

**IN THE UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
OAKLAND DIVISION**

CHASOM BROWN, *et al*, individually  
and on behalf of all others similarly  
situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 5:20-cv-03664-YGR

**EXPERT REPORT OF PROFESSOR ON AMIR**

**APRIL 15, 2022**

**CONFIDENTIAL**  
**SUBJECT TO PROTECTIVE ORDER**



*CONFIDENTIAL*  
*SUBJECT TO PROTECTIVE ORDER*

## Table of Contents

<b>I. EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>II. QUALIFICATIONS .....</b>	<b>6</b>
<b>III. ASSIGNMENT.....</b>	<b>7</b>
<b>IV. BACKGROUND .....</b>	<b>9</b>
A. Allegations .....	9
B. Private Browsing Mode .....	11
C. Relevant Policies and Disclosures .....	15
<b>V. CONSUMER PREFERENCES FOR BROWSERS AND BROWSER FEATURES VARY, AND CONSUMER PERCEPTIONS AND EXPECTATIONS OF PRIVACY ARE CONTEXT SPECIFIC .....</b>	<b>18</b>
A. Consumer Preferences of Browsers and Browser Features Vary .....	18
B. Consumers' Concerns About Privacy Depend on The Context.....	20
<b>VI. CONSUMER PERCEPTIONS AND EXPECTATIONS STUDY .....</b>	<b>22</b>
A. Study Design.....	23
B. Analysis and Results .....	24
<b>VII. INTERPRETATION STUDY.....</b>	<b>28</b>
A. Study Design.....	28
B. Analysis and Results .....	30
<b>VIII. LIKELIHOOD OF USE STUDY .....</b>	<b>35</b>
A. Study Design.....	36
B. Analysis and Results .....	40

**I. EXECUTIVE SUMMARY**

1. Based on my experience, the materials I reviewed in this matter, and the studies I designed and conducted in this case, I have reached the following opinions:

**Opinion 1 (See Section V)**

2. Literature shows that consumer preferences vary when it comes to internet browsers and browser features.<sup>1</sup> This variation in preferences is dependent on the context and scenario, such as *which* people or entities have access to consumer information, *what* types of consumer information people or entities have access to, and *how* people or entities use this consumer information. Therefore, to evaluate consumer understanding, perceptions, and expectations specific to the facts of this case, and to evaluate whether and to what extent consumers' understanding, perceptions, and expectations affect their likelihood of using a specific internet browser or browser feature, I designed and conducted empirical studies to address my assignment in a way that is consistent with the facts and context relevant to it.

**Opinion 2 (See Section VI)**

3. I designed and conducted my Consumer Perceptions and Expectations Study to assess whether and to what extent users expect different types of entities to receive or to not receive data (such as IP address, URLs of the sites users visit, and cookies) when they visit websites while in private browsing mode.<sup>2</sup> Users' perceptions and expectations were assessed after viewing the private browsing splash screens for Chrome, Safari, or Firefox, as well as the "Learn More" pages that are linked to the Chrome and Firefox private browsing splash screens.
4. In this study, my target population consists of 500 adults residing in the US who use a private browsing mode. Respondents were assigned to one of three groups (with a minimum of 200 respondents in the Chrome group, a minimum of 50 respondents in the Safari group, and a minimum of 50 respondents in the Firefox group) based on their answers to the screening question regarding the internet browser(s) they currently use to browse the internet.<sup>3</sup> Respondents were then presented with the private browsing splash

---

<sup>1</sup> See **Section V** for a review of the literature.

<sup>2</sup> See footnote 11 in **Section III** for rationale on the types of data tested.

<sup>3</sup> QS7, "Thinking about the device(s) you use to browse the internet (such as your phone, your personal laptop, or your office computer), which internet browser(s) do you currently use? (*Select all that apply*).” See **Appendix F.1**.

CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

screens for Chrome, Safari, or Firefox, as well as with the “Learn More” pages that are linked to the Chrome (for those in the Chrome group) and Firefox (for those in the Firefox group) private browsing splash screens. Respondents were asked to express their understanding of whether and to what extent the three enumerated entities receive or do not receive data (such as IP address, URLs of the sites visited, and cookies) when they visit websites while in private browsing mode. The types of entities were companies that provide analytics and advertising services to websites visited, internet service providers, or companies that own the websites visited.

5. My Consumer Perceptions and Expectations Study shows that, overall, respondents expect that companies that provide analytics and advertising services to websites visited, internet service providers, and companies that own the websites visited *receive* data from their private browsing session (such as IP address, URLs of the sites visited, and cookies). Around half of the respondents in the Chrome group (44% to 53%) expect that companies that provide analytics and advertising services to websites visited, internet service providers, and companies that own the websites visited *probably* or *do* receive the data from their private browsing session.
6. Only 15% to 20% of respondents in the Chrome group expect that companies that provide analytics and advertising services to websites visited, internet service providers, and companies that own the websites visited *do not* receive the data from their private browsing session. Even including respondents who answered *probably do not* receive, 26% to 35% of respondents in the Chrome group expect that these entities *do not* or *probably do not* receive the data from their private browsing session. Results are similar when analyzing responses from respondents across all three internet browsers.
7. These findings are not consistent with Plaintiffs’ claim that “Class members reasonably believed that their data would not be collected by Google and that Google would not intercept their communications when they were in ‘private browsing mode.’”<sup>4</sup>

---

<sup>4</sup> Third Amended Complaint, *Chasom Brown, et al., Plaintiffs, v. Google LLC, Defendant*, United States District Court, Northern District of California – Oakland Division, No. 5:20-cv-03664-YGR, February 3, 2022 (“TAC”), ¶ 3.

**Opinion 3 (See Section VII)**

8. I designed and conducted my Interpretation Study to assess whether and to what extent users expect Google to receive or to not receive URLs of the sites users visit, IP addresses, and cookies placed on users' browsers during their Incognito session after reviewing the Incognito Splash Screen and "Learn More" page, as well as the Google Privacy Policy and Chrome Privacy Notice, the New Account Creation Agreement, or the Consent Bump Agreement for some respondents.<sup>5,6</sup>
9. In this study, my target population consists of 1,000 adults residing in the US who use a private browsing mode. Respondents were randomly assigned to one of four groups with a target of 250 respondents per group. The four groups were presented with different sets of screens and policies: "Splash Screen Only," "Splash Screen with Policies (Highlighted)," "Splash Screen with New Account Creation Agreement," and "Splash Screen with Consent Bump Agreement and FAQ Page." All respondents were shown the Incognito Splash Screen and the "Learn More" page that is linked to the Incognito Splash Screen. Based on which group they were assigned to, respondents were also shown either no additional documents (Splash Screen Only group), the Google Privacy Policy and the Chrome Privacy Notice (with and without highlights) (Splash Screen with Policies (Highlighted) group), the New Account Creation Agreement (Splash Screen with New Account Creation Agreement group), or the Consent Bump Agreement and FAQ Page (Splash Screen with Consent Bump Agreement and FAQ Page). Each respondent was asked a series of three scale questions. These questions required respondents to express their understanding of whether Google receives or does not receive three types of data from their Incognito mode internet browsing session: URLs of the sites visited, IP addresses, and cookies placed on the browser.
10. My Interpretation Survey results show that, overall, respondents expect that Google receives the URLs of the sites visited, IP addresses, and cookies placed on the browser while in Incognito mode. Over half of respondents in each group (52% to 55%) expect that Google *probably* receives or *does* receive URLs of the sites visited while in Incognito

---

<sup>5</sup> See footnote 11 in **Section III** for rationale on the types of data tested.

<sup>6</sup> See **Section IV.C** for descriptions of the policies and disclosures.

mode, over half of respondents in each group (62% to 65%) expect that Google *probably* receives or *does* receive IP addresses while in Incognito mode, and close to half of respondents in each group (46% to 55%) expect that Google *probably* receives or *does* receive cookies placed on the browser while in Incognito mode.

11. In each group, only 13% to 19% of respondents expect that Google *does not* receive URLs of the sites visited while in Incognito mode, 6% to 12% of respondents expect that Google *does not* receive IP addresses while in Incognito mode, and 17% to 25% of respondents expect that Google *does not* receive cookies placed on the browser while in Incognito mode. Even including respondents who answered *probably does not* receive, 25% to 29% respondents expect that Google *does not* or *probably does not* receive the URLs of sites visited while in Incognito mode. The percentage of respondents that expect that Google *does not* or *probably does not* receive (1 or 2 on the scale) IP addresses is 14% to 20% and for cookies placed on the browser is 29% to 38%.
12. These findings are not consistent with Plaintiffs' claim that "[n]othing in Google's Privacy Policy or Incognito Screen leads users to believe that during private browsing Google continues to persistently monitor them [...] In fact, when the Privacy Policy and Incognito Screen are read together, the user necessarily reaches the opposite conclusion."<sup>7</sup>

#### **Opinion 4 (See Section VIII)**

13. I designed and conducted my Likelihood of Use Study to assess whether and to what extent modification of certain language on the Incognito Splash Screen and the "Learn More" page that address Plaintiffs' criticisms of those documents—namely, that these documents should have identified Google as an entity that may receive data when an Incognito user visits a website using Google services—impacts users' likelihood of using Chrome in Incognito mode for private browsing.
14. Because this survey is about users' actual behavior and because context matters, I presented a scenario to simulate the browsing experience. This scenario was the same across all respondents. This scenario asked respondents to imagine that they were researching online about a sensitive topic and they decided to browse the web in private browsing mode.

---

<sup>7</sup> TAC, ¶ 57.

15. In this study, my target population consists of 1,000 adults residing in the US who use a private browsing mode. I used a test/control experimental design, where respondents were randomly assigned to either the Actual Language group or the Alternative Language group, with a target of 500 respondents in each group. Following the presentation of the scenario, respondents were shown either the actual version of the Incognito Splash Screen (Actual Language group), or the alternative version with modification of certain language (Alternative Language group). Specifically, in the alternative version of the Incognito Splash Screen, the introductory sentence, “Now you can browse privately, and other people who use this device won’t see your activity” was modified to say, “Now you can browse privately, which means other people who use this device won’t see your activity.” Similarly, under the heading, “Your activity might still be visible to,” I added a bullet that stated: “Companies that provide services to websites you visit (such as Google Analytics, Adobe Analytics, Google Ad Manager, Facebook Ads).”<sup>8</sup> These language modifications address Plaintiffs’ allegations as to how the actual language in the Incognito Splash Screen allegedly is misleading. Respondents that clicked the link to the “Learn More” page on the Incognito Splash Screen saw either actual or alternative language depending on the condition to which they were assigned. After viewing the stimuli, respondents were asked how likely or unlikely they were to use the Chrome browser in Incognito mode to do online research on a sensitive topic.
16. My Likelihood of Use Study results show that for online research on a sensitive topic, the average respondent would use Chrome in Incognito mode to do online research on a sensitive topic after viewing the Incognito Splash Screen and for some respondents, the “Learn More” page. Importantly, modifying certain language on the Incognito Splash Screen and the “Learn More” page (*i.e.*, the second phrase in the introductory sentence and information regarding the list of entities to which users’ activity might still be visible) to address Plaintiffs’ criticisms regarding what those documents *should* disclose *has no statistically significant impact* on respondents’ likelihood of using Chrome in Incognito mode to do online research on a sensitive topic. This finding shows that including language that Plaintiffs claim “Google could have disclosed on [the] Incognito Screen [to describe]

---

<sup>8</sup> See **Appendices H.1 and H.2.**

*CONFIDENTIAL*  
*SUBJECT TO PROTECTIVE ORDER*

that Google would track users and collect their data while they were browsing privately”<sup>9</sup>  
does not have an impact on respondents’ likelihood of using Chrome.

## **II. QUALIFICATIONS**

17. I am the Wolfe Family Presidential Endowed Chair in Life Sciences, Innovation, and Entrepreneurship, and Professor of Marketing at the Rady School of Management, University of California, San Diego. I have been a professor of marketing for the past nineteen years. I received my PhD in Management Science and Marketing from the Massachusetts Institute of Technology in 2003. From 2003 to 2005, I was an Assistant Professor of Marketing at Yale University. In 2005, I moved to help found the Rady School of Management at UC San Diego, where I was the first founding member of the marketing department and have served as an associate dean of academic programs.
18. I have taught Marketing Management, Pricing, Consumer Behavior, Business Analytics, Marketing Strategy, Market Research, Applied Market Research, Lab to Market, and Data Driven Decision Making at the MBA and Executive levels, as well as many specific programs for major corporations (both nationally and internationally). I have also taught MBA Marketing Management courses at Northwestern University’s Kellogg School of Management, Yale School of Management, Recanati School of Business of Tel Aviv University, IDC Herzelia, and Cheung Kong Graduate School of Business in Shanghai, China.
19. I have consulted with numerous companies in many industries on topics relating to market analysis, market research, business strategy, customer insights, branding, customer analysis, new product launches, pricing, promotions, and customer relationship management. I am also the Chief Behavioral Science Officer at Fiverr, Inc and serve on the advisory board of several companies.
20. I have published numerous highly cited and award-winning articles in leading marketing, management, and psychology journals, and I am often invited to lecture in leading business school and professional meetings. I have also designed and conducted hundreds of consumer surveys, both for my academic research and consulting work. My professional

---

<sup>9</sup> TAC, ¶ 53.



qualifications are described further in my curriculum vitae, which is attached as **Appendix A**.

21. I have also served as an expert witness in several cases, including consumer protection class actions. **Appendix B** lists matters where I have testified as an expert witness. I have also been retained on several cases that either settled or are ongoing.
22. My rate of compensation for this assignment is \$900 per hour. Individuals at Analysis Group, Inc., an economic and litigation consulting firm headquartered in Boston, Massachusetts, performed part of the work for this assignment under my direction. No compensation is contingent upon the outcome of this research or of the case.

### III. ASSIGNMENT

23. I have been asked by Counsel for Google LLC (“Google”) to evaluate the understanding, perceptions, and expectations of users with respect to issues relevant to the matter (see **Section IV**). In accordance with my assignment, I conducted a series of surveys specific to the facts of this matter.<sup>10</sup> In particular, I was asked to assess the following:
  - a. Whether and to what extent users expect different types of entities to receive or to not receive data (such as IP address, URLs of the sites users visit and cookies)<sup>11</sup> when they visit websites while in private browsing mode after viewing the private browsing splash screens for Chrome, Safari, or Firefox, as well as the “Learn More” pages that are linked to the Chrome and Firefox private browsing splash screens. (**Consumer Perceptions and Expectations Study**, see **Section VI**.)
  - b. Whether and to what extent users expect Google to receive or to not receive URLs of the sites users visit, IP addresses, and cookies placed on the browser during their Incognito session after reviewing the Incognito Splash Screen and “Learn More” page, as well as the Google Privacy Policy and Chrome Privacy

---

<sup>10</sup> Surveys are widely utilized in academic research and in litigation. See Lavrakas, Paul J., *Encyclopedia of Survey Research Methods*, SAGE Publications, Inc., 2008, p. 33; Ben-Shahar, Omri and Lior J. Strahilevitz, “Interpreting Contracts Via Surveys and Experiments,” *New York University Law Review*, Vol. 92, 2017, pp. 1753-1827 (“Ben-Shahar and Strahilevitz (2017)”), pp. 1769-1771.

<sup>11</sup> I am informed that URLs of the sites visited, IP address, and cookies broadly cover the data types at issue in this case, and these three types of data are relatively understandable concepts for survey respondents (see **Section IV.A** for the list of data types at issue). Further, testing too many types of data may cause fatigue for respondents. Therefore, testing these three types of data is appropriate for my assignment.



Notice, the New Account Creation Agreement, or the Consent Bump Agreement for some respondents. (**Interpretation Study**, see **Section VII.**)

- c. Whether and to what extent modification of certain language on the Incognito Splash Screen and “Learn More” page impacts users’ likelihood of using Chrome in Incognito mode for private browsing. (**Likelihood of Use Study**, see **Section VIII.**)

24. In designing the surveys and analyzing the results, I follow professional standards and best practices of conducting survey research, both generally and specifically for the purpose of litigation.<sup>12,13</sup>
25. I may amend or supplement my opinions should additional information be made available following the submission of my report through incremental document and data production or deposition testimony. In formulating my opinions, I considered the materials cited in this report and listed in **Appendix C.**

---

<sup>12</sup> My survey approach adhered to the survey research guidelines outlined by the Federal Judicial Center in the “Reference Guide on Survey Research” and in the “Manual for Complex Litigation,” sources that are foundational for litigation survey design. Diamond, Shari S., “Reference Guide on Survey Research,” in *Reference Manual on Scientific Evidence*, Third Edition, 2011, The National Academies Press, pp. 359-423 (“Diamond (2011)”); *Manual for Complex Litigation*, Fourth Edition, Federal Judicial Center, 2004 (“Manual for Complex Litigation”).

The Manual for Complex Litigation describes the following criteria for a reliable study: (1) the population was properly chosen and defined; (2) the sample chosen was representative of that population; (3) the survey was conducted by qualified people following proper interview procedures; (4) the questions asked were clear and not leading; (5) the data gathered were accurately reported; (6) the data were analyzed in accordance with accepted statistical principles; and (7) the process was conducted to ensure objectivity. Manual for Complex Litigation, p. 103.

To ensure objectivity and to avoid “demand artifacts” (*i.e.*, elements of the methodology or survey that may lead the respondent to answer in a particular way), I followed best practices in survey design. My survey followed “double-blind” methodology where both respondents and the survey administrator (in this case, Dynata, a reputable survey vendor) were not provided information on the purpose or sponsor of this study. By following a “double-blind” methodology, I avoided respondents answering in the way that the respondent thinks the survey designer “demanded.” I also minimized demand artifacts through my design of the survey questions and answers. For example, I asked questions in a double-sided manner (*e.g.*, “how likely or unlikely...”) where appropriate to avoid leading respondents to answer one way over another. Furthermore, I mitigated order effects by rotating or randomizing the order of questions and answer alternatives where appropriate, as well as randomizing the order of stimuli. Sawyer, Alan G., “Demand Artifacts in Laboratory Experiments in Consumer Research,” *Journal of Consumer Research*, Vol. 1, No. 4, 1975, pp. 20-30; Diamond (2011), pp. 395-396, 410-411. *See also*, Miller, Jeff, “Online Marketing Research,” in *The Handbook of Marketing Research*, Grover, Rajiv and Marco Vriens, eds., Sage Publications, 2006, pp. 110-131.

<sup>13</sup> Pretesting is recommended “as a way to increase the likelihood that questions are clean and unambiguous.” Diamond (2011), p. 388. Under my direction, pretests were conducted for my surveys from March 4<sup>th</sup>, 2022 to March 10<sup>th</sup>, 2022. Respondents were asked to complete the survey while “thinking out loud” and to answer a set of follow-up questions about the survey experience. 10 respondents were interviewed for each of my surveys. Based on the results of pretesting, which are shown in more detail in **Appendix E**, I was able to refine each of my surveys.

In response to confusion about whether the hyperlink worked when respondents clicked on “Learn more” on the private browsing splash page, I added a pop-up text box to the survey when the hyperlink was clicked that says “You will be taken to the next page in [X] seconds” where X mirrors the number of seconds remaining in the 30-second time for each page. These stimuli are discussed in more detail in **Sections IV.C, VI.A, VII, A., and VIII.A** below. Additionally, in response to issues with scrolling while using the zoom feature available for my stimuli, I added an instruction to “please drag the image to scroll.”

**IV. BACKGROUND****A. Allegations**

26. I understand that Chasom Brown, William Byatt, Jeremy Davis, Christopher Castillo, and Monique Trujillo (collectively “Plaintiffs”), on behalf of a proposed Class, allege in the Third Amended Complaint (“TAC”) that, among other things, Google “intercepted users’ private browsing communications to collect personal and sensitive information concerning millions of Americans, without disclosure and consent” while users are in a “private browsing mode.”<sup>14</sup>
27. Plaintiffs acknowledge that they understood Google collected the At-Issue Data when they were browsing the web when in a mode other than private browsing mode. Indeed, they allege that “[i]t is common knowledge that Google collects information about the web-browsing activity of users who are not in ‘private browsing mode’” and that “[i]t is also common knowledge that Google causes targeted advertisements to be sent based on that information.”<sup>15</sup> Plaintiffs also affirmed this belief at their depositions.<sup>16</sup>
28. I understand that, because Plaintiffs acknowledge that users generally understand that Google collects the At-Issue Data when they were in a mode other than private browsing mode, a key issue in the case is whether certain of Google’s statements in its disclosures

---

<sup>14</sup> TAC, ¶¶ 1, 4.

<sup>15</sup> TAC, ¶ 163.

<sup>16</sup> “Q. How do you know that Google collects information and monetizes that information? A. It’s common knowledge, I think. I don’t know how to say that more specifically, but I think everyone knows that that’s Google’s business model.” Zoom Videotaped Deposition of William Byatt, December 20, 2021 (“Byatt Deposition”), at 153:15-21; “Q. And do you agree, as someone who works in the space that you work in, that it is — it’s common knowledge that Google collects information about web browsing activity when people are not in private mode? A. Yeah, I would say that’s a fair statement.” Video-Recorded Deposition of Jeremy Davis, January 7, 2022 (“Davis Deposition”), at 69:10-14; “I don’t assume privacy in, quote/unquote, ‘normal Chrome sessions.’ Why else would the incognito mode exist and why else would the Privacy Policy refer to it as the prescribed way to browse privately?” Davis Deposition, at 70:23-71:2; “It’s clear to me that when I’m searching Google in regular mode, and not Incognito mode, that you collect this data.” Videotaped Deposition of Christopher Castillo, February 8, 2022 (“Castillo Deposition”), at 70:12-14; “I understand when I am not in Incognito mode that Google will intercept my communications [...] it’s my understanding that Google collects that kind of data when I am not in Incognito mode, per the statements that are written in the Google Privacy Policy.” Castillo Deposition, at 100:3-25; “And because I understand that, hey, if I go do normal browsing, I’m doing normal browsing and I’m giving up data and...my data’s being collected, and that’s the deal we have.” Videotaped Deposition of Chasom Brown, January 13, 2022 (“Brown Deposition”), at 61:2-5; “I don’t hate the idea of data collection in normal Chrome browsing.” Brown Deposition, at 82:7-8; “I’m just using Google in normal mode, I think there is still quite a bit that’s being collected.” Brown Deposition, at 134:8-10; “[I]n general, I think targeted advertising is a good thing. And normal browsing mode, I think that, again, it’s I’ve given consent. We have a deal. I get the deal.” Brown Deposition, at 158:8-11; “Well, if I’m in regular mode, then I am aware that information is being collected.” Virtual Videoconference Video-Recorded Deposition of Monique Trujillo, February 11, 2022 (“Trujillo Deposition”), at 56:11-12; “I know that in regular mode I am consenting to Google Analytics collecting my information.” Trujillo Deposition, at 62:12-14.

led Class Members to believe that Google would not receive the At-Issue Data while users were in a private browsing mode.

29. Plaintiffs allege that “[b]ased on Google’s representations, Plaintiffs and Class members reasonably believed that their data would not be collected by Google and that Google would not intercept their communications when they were in ‘private browsing mode.’”<sup>17</sup> Plaintiffs allege that Google intercepted and collected data “through means that include Google Analytics, Google ‘fingerprinting’ techniques, concurrent Google applications and processes on a consumer’s device, and Google’s Ad Manager.”<sup>18</sup>
30. Plaintiffs state that

Whenever a user (even a user in “private browsing mode,” including Plaintiffs and Class members) visits a website that is running Google Analytics or Google Ad Manager, Google’s software scripts on the website surreptitiously direct the user’s browser to send a secret, separate message to Google’s servers in California. This message contains:

- a. The “GET request” sent from the user’s computer to the website.<sup>19</sup> [...]
- b. The IP address of the user’s connection to the internet;<sup>20</sup>
- c. Information identifying the browser software that the user is using, including any “fingerprint” data;<sup>21</sup>
- d. Any “User-ID” issued by the website to the user, if available [...];<sup>22</sup>
- e. Geolocation of the user, if available [...];<sup>23</sup> and

---

<sup>17</sup> TAC, ¶ 3.

<sup>18</sup> TAC, ¶ 8.

<sup>19</sup> The Complaint defines “GET request” as, “When an individual internet user visits a web page, his or her browser sends a message called a ‘GET request’ to the webpage’s server. The GET request serves two purposes: it first tells the website what information is being requested and then instructs the website to send the information back to the user [...] The GET request also transmits a refer[r]er header containing the URL information of what the user has been viewing and requesting from websites online.” TAC, ¶ 63. I am informed that “URLs of the sites visited” is a more understandable concept for survey respondents. Thus, I presented the term, “URLs of the sites you visit,” with the following definition: “The web addresses of the webpages you visited using the browser.” **Appendices F.1 and F.2.**

<sup>20</sup> The Complaint defines “IP address” as, “Each device, when connected to the Internet, is assigned a unique IP address by the Internet Service Provider (ISP) that is providing the internet connection. IP addresses may change over time but often do not. In many cases, an ISP will continue to assign the same IP address to the same device.” TAC, ¶ 63, footnote 16. The definition I presented in my surveys is, “Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. An IP address can often be used to identify the location from which a device is connecting to the Internet.” **Appendices F.1 and F.2.**

<sup>21</sup> The Complaint defines “fingerprint data” as, “Because every device and application installed has small differences, images, digital pixels, and fonts display differently for every device and application, just ever so slightly. By forcing a consumer to display one of its images, pixels, or fonts, online companies such as Google are able to ‘fingerprint’ their users and consumers across the internet.” TAC, ¶ 100.

<sup>22</sup> The Complaint defines “User-ID” as, “The User-ID feature allows Websites to ‘generate [their] own unique IDs, consistently assign IDs to users, and include these IDs wherever [the Websites] send data to Analytics.’” TAC, ¶ 69. *See also*, “About the User-ID Feature,” *Google Analytics Help*, available at <[https://support.google.com/analytics/answer/3123662?hl=en&ref\\_topic=3123660](https://support.google.com/analytics/answer/3123662?hl=en&ref_topic=3123660)>, accessed on March 18, 2022.

<sup>23</sup> The Complaint describes “geolocation” as information on the location of a user’s device which can be captured by Google via any device that uses its software (Android, Google Home, Nest, etc.). *See* TAC, ¶ 105-108.

- f. Information contained in “Google cookies,” which were saved by the user’s web browser on the user’s device at any prior time.<sup>24</sup>

31. I collectively refer to these data as “At-Issue Data.”
32. Plaintiffs assert that Plaintiffs’ and Class members’ expectation of privacy is based on “Google’s own statements regarding ‘private browsing modes.’”<sup>25</sup>
33. Plaintiffs make these allegations on behalf of a class (“Proposed Class”) defined as:

Class 1 – All Chrome browser users with a Google account who accessed a non-Google website containing Google tracking or advertising code using such a browser and who were (a) in “Incognito mode” on that browser and (b) were not logged into their Google account on that browser, but whose communications, including identifying information and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present (the “Class Period”).

Class 2 – All non-Chrome browser users with a Google account who accessed a non-Google website containing Google tracking or advertising code using any such browser and who were (a) in “private browsing mode” on that browser, and (b) were not logged into their Google account on that browser, but whose communications, including identifying information and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present (the “Class Period”).<sup>26</sup>

## B. Private Browsing Mode

### 1. Incognito Mode of Chrome

34. Chrome is an internet browsing software application developed by Google.<sup>27</sup> Although it is one of many browser options (with some alternatives being Safari, Firefox, Edge, Opera, Brave, and DuckDuckGo), Chrome is the most widely used internet browser across all device types (*e.g.*, desktop, tablet, and mobile) as of 2022.<sup>28</sup> “Incognito” mode is one of the five browsing modes available for Chrome users to choose from and is the private

---

<sup>24</sup> The Complaint defines cookies as “A ‘cookie’ is a piece of code that records information regarding the state of the user’s system (*e.g.*, username; other login information; items added to a “shopping cart” in an online store) or information regarding the user’s browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past). Cookies can also be used to remember pieces of information that the user previously entered into form fields, such as names, addresses, passwords, and payment card numbers.” TAC, ¶ 70, footnote 19. The definition I presented in my surveys is, “A small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information.” **Appendices F.1 and F.2.**

<sup>25</sup> TAC, ¶¶ 39-62.

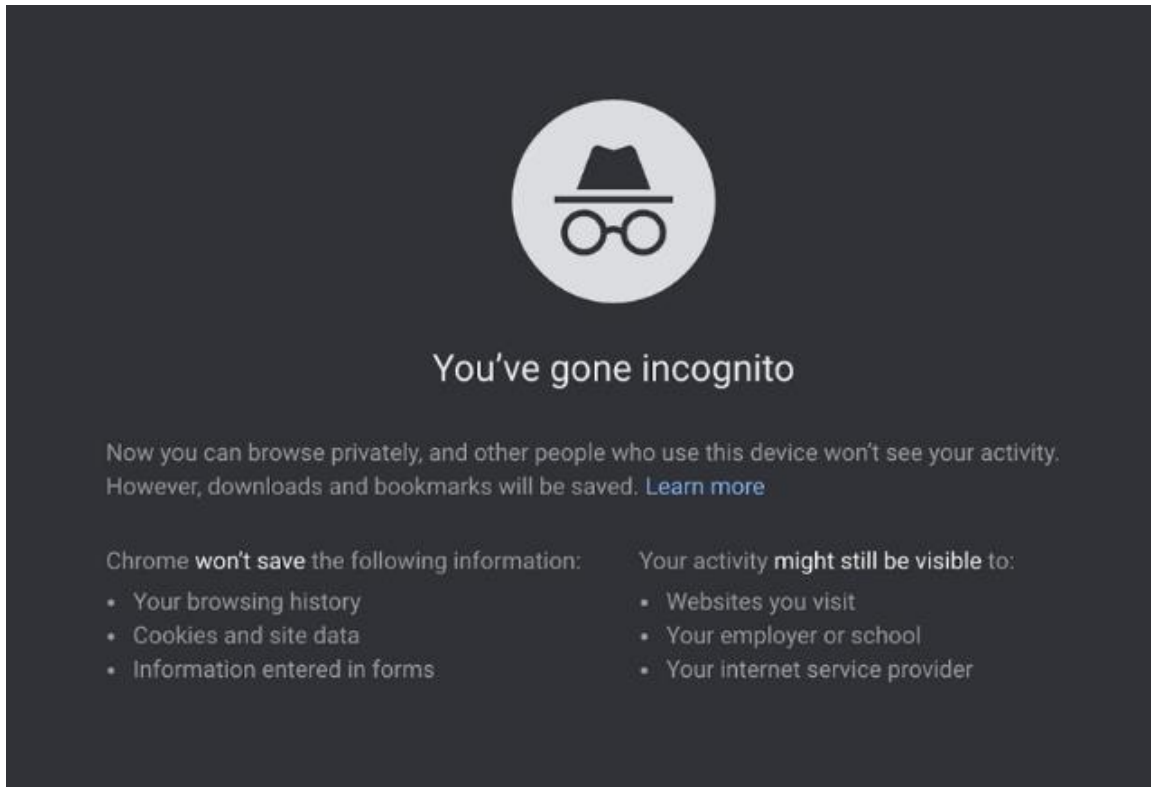
<sup>26</sup> TAC, ¶ 192.

<sup>27</sup> “Google Chrome - Home,” *Google*, available at <<https://www.google.com/chrome/>>, accessed on March 18, 2022.

<sup>28</sup> “Browser Market Share Worldwide,” *StatCounter*, available at <<https://gs.statcounter.com/browser-market-share#yearly-2009-2022>>, accessed on March 18, 2022.

browsing mode of the Chrome browser.<sup>29,30</sup> **Figure 1** below shows what was displayed when a user initiated Incognito mode on Chrome during the majority of the class period (this initial display is also known as a “splash screen”).<sup>31, 32</sup>

**Figure 1. Chrome Browser Incognito Mode Splash Screen**



35. As **Figure 1** shows, the Incognito Splash Screen states that, in Incognito mode, Chrome will not save the user’s browsing history, cookies and site data, or information entered in forms. Google further explains in the Chrome Privacy Notice that, after the user closes the Incognito session, Chrome also will not save data including snapshots of visited pages, or records of downloads locally on the user’s browser.<sup>33</sup>

<sup>29</sup> The five browsing modes are (1) basic browser mode, (2) sign in without sync enabled, (3) sign in with Sync enabled, (4) Incognito mode, and (5) guest mode. See “Chrome Privacy Notice,” May 20, 2020, *Google*, available at <<https://www.google.com/chrome/privacy/archive/20200520/>>. See also, **Appendices N.1 and N.2**.

<sup>30</sup> “Browse in Private,” *Google*, available at <<https://support.google.com/chrome/answer/95464?hl=en>>, accessed on March 18, 2022.

<sup>31</sup> TAC, ¶ 52.

<sup>32</sup> Shortly before the Plaintiffs filed the Complaint, Google launched Chrome version 83 which blocked third-party cookies by default in Incognito mode, and added a toggle to the “splash screen” informing users that when it was on, sites could not use cookies that track them across the web, but that features on sites may break. See TAC, ¶ 139. See also, “M83 Chrome Enterprise Release Notes,” May 19, 2020, *Chrome Enterprise*, available at <<https://support.google.com/chrome/a/answer/10314655#83>>. I chose to use the version of the Incognito Splash Screen that existed for the majority of the class period, and that was used in the Complaint.

<sup>33</sup> “Chrome Privacy Notice,” May 20, 2020, *Google*, available at <<https://www.google.com/chrome/privacy/archive/20200520/>>.



36. The Chrome Privacy Notice also explains that in Incognito mode, “Chrome won’t share existing cookies with sites [users] visit in incognito [...] mode.”<sup>34</sup> Although “[s]ites may deposit new cookies on [the user’s] system [...], [...] they’ll only be stored and transmitted until [the user] close[s] the[ir] last incognito window,” at which point they are automatically deleted from the browser.<sup>35,36</sup> While browsing in Incognito, users “have access to information from [their] existing profile, such as suggestions based on [their] browsing history and saved passwords.”<sup>37</sup>
37. The Incognito Splash Screen and other Google disclosures state that, in Incognito mode, users’ activity is not completely private and may still be visible to websites they visit, their employer or school, or their internet service provider. (See **Figure 1.**) Google’s Help Center article titled “How private browsing works in Chrome” explains that users’ activity may also still be visible to ads and resources used on the websites they visit, websites they sign in to, or search engines.<sup>38</sup>

## 2. Private Browsing Mode of Other Browsers

38. Other popular internet browsers also provide private browsing modes. For example, Safari and Firefox, the second and third most widely used internet browsers respectively as of February 2022, also each have their own private browsing modes.<sup>39</sup> **Figure 2** and **Figure 3** below show the splash screens displayed when a user initiates private browsing mode on Safari’s browser or Firefox’s browser.

---

<sup>34</sup> “Chrome Privacy Notice,” May 20, 2020, *Google*, available at <<https://www.google.com/chrome/privacy/archive/20200520/>>. See also, **Appendices N.1 and N.2.**

<sup>35</sup> “Chrome Privacy Notice,” May 20, 2020, *Google*, available at <<https://www.google.com/chrome/privacy/archive/20200520/>>. See also, **Appendices N.1 and N.2.**

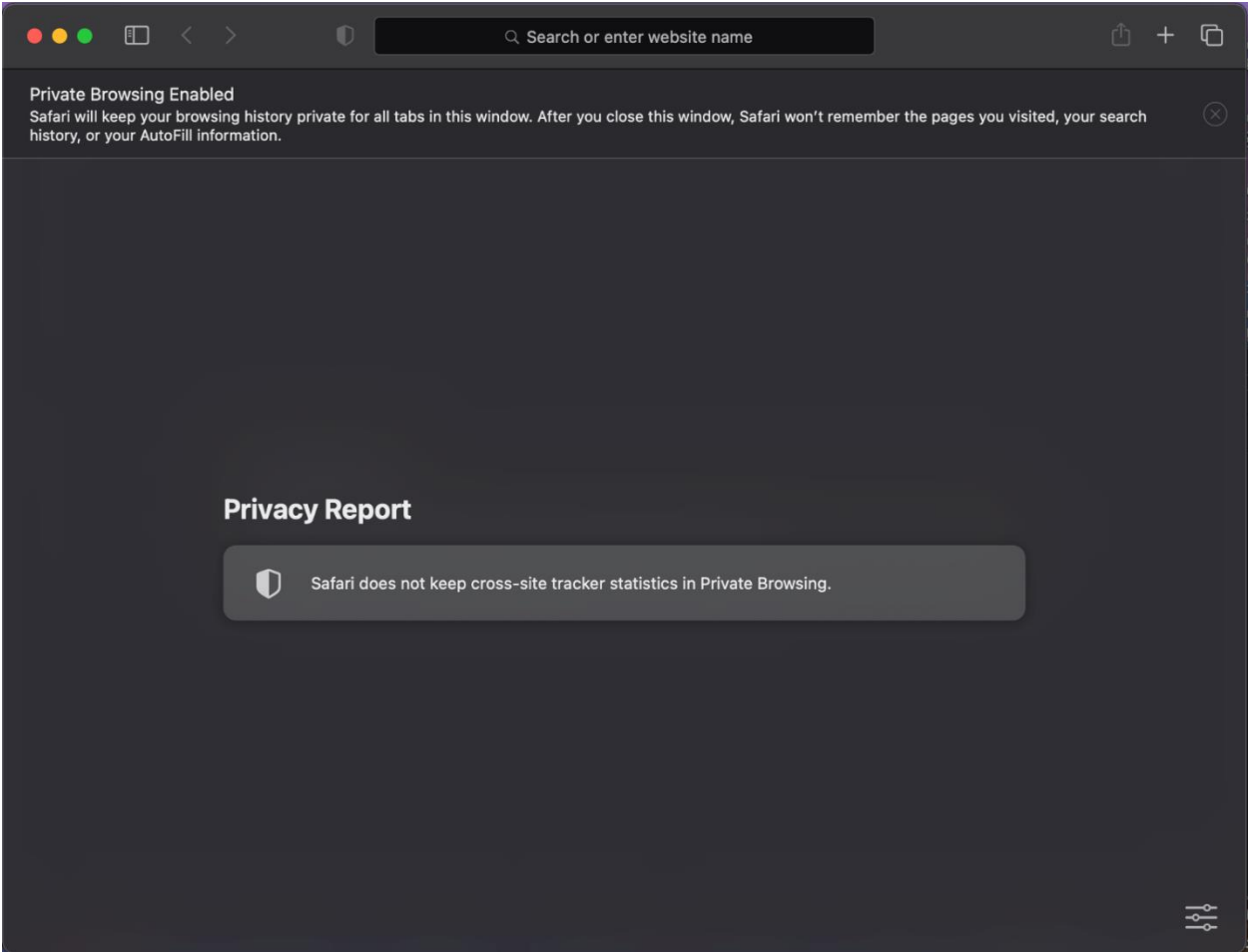
<sup>36</sup> “How Private Browsing Works in Chrome,” *Google*, available at <[https://support.google.com/chrome/answer/7440301?hl=en&ref\\_topic=9845306](https://support.google.com/chrome/answer/7440301?hl=en&ref_topic=9845306)>, accessed on March 18, 2022. See also, **Appendix I.1.**

<sup>37</sup> “Chrome Privacy Notice,” May 20, 2020, *Google*, available at <<https://www.google.com/chrome/privacy/archive/20200520/>>. See also, **Appendices N.1 and N.2.**

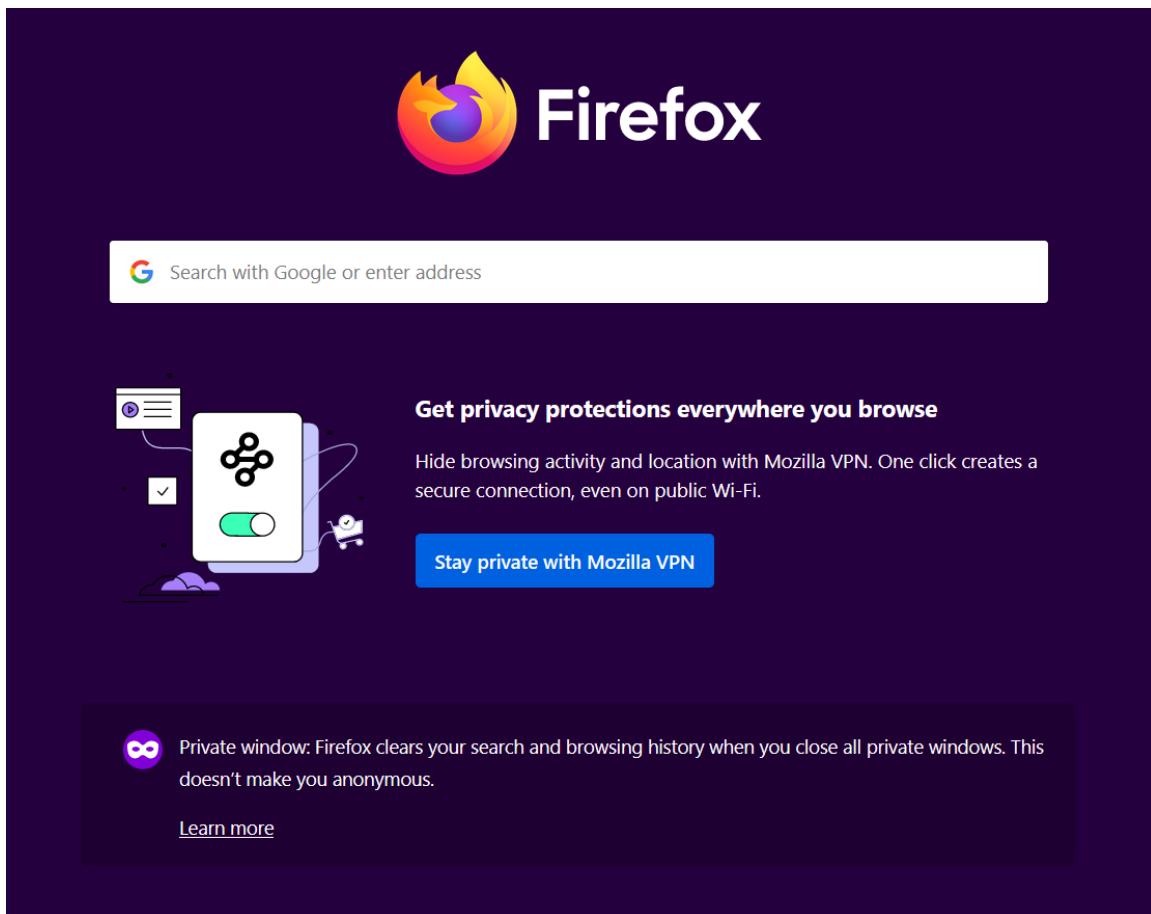
<sup>38</sup> “How Private Browsing Works in Chrome,” *Google*, available at <[https://support.google.com/chrome/answer/7440301?hl=en&ref\\_topic=9845306](https://support.google.com/chrome/answer/7440301?hl=en&ref_topic=9845306)>, accessed on March 18, 2022. See also, **Appendix I.1.**

<sup>39</sup> “Browser Market Share Worldwide,” *StatCounter*, available at <<https://gs.statcounter.com/browser-market-share#yearly-2009-2022>>, accessed on March 18, 2022.

Figure 2. Safari Browser Private Browsing Mode Splash Screen



39. The Private Browsing Splash Screen of Safari’s browser states that “Safari will keep your browsing history private for all tabs in this window. After you close this window, Safari won’t remember the pages you visited, your search history, or your AutoFill information.” (See **Figure 2.**)

**Figure 3. Firefox Browser Private Browsing Mode Splash Screen**

40. The Private Browsing Splash Screen of Firefox’s browser states “Private window: Firefox clears your search and browsing history when you close all private windows. This doesn’t make you anonymous.” (See **Figure 3**).

### C. Relevant Policies and Disclosures

41. I am informed that the following policies and disclosures to the Class members are relevant in this case:
- a. ***Incognito Splash Screen:*** The Incognito Splash Screen appears when a user opens an Incognito browsing session in the Chrome browser. It provides information on the type of information that the user’s Chrome browser will not save in Incognito mode (as opposed to regular mode) and explains that Incognito mode does not conceal the user’s activity from certain types of entities.<sup>40</sup> (See **Figure 1** and **Section III.A.1**).
  - b. ***“Learn More” Page:*** The “Learn More” page is hyperlinked to the Incognito Splash Screen and provides additional information on “[h]ow private browsing works on Chrome” including that “other people who use the device won’t see your

<sup>40</sup> I am informed that the version of the Incognito Splash Screen that was used by Plaintiffs in the TAC is relevant for my report. TAC, ¶ 52. See also, **Appendix H.1**.



CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

history” and “[c]ookies and site data are remembered while you’re browsing, but deleted when you exit Incognito mode.” The page also explains that “[y]our activity, like your location, might still be visible to: [[w]ebsites you visit, including the ads and resources used on those sites[,] [w]ebsites you sign in to [...] [and] [s]earch engines.”<sup>41</sup>

- c. **Google Privacy Policy (“PP”)**: Google’s PP explains to users, among other things, the types of information Google collects and how the data is stored and used. Specifically, the PP explains the types of data Google receives, including unique identifiers, browser type and settings, device types and settings, operating system, mobile network information, application version number, IP address, system activity, and referrer URL, and how that data is stored depending on whether or not the user is signed-in to a Google Account. The PP also explains that Google uses this data to provide and improve its services, to provide personalized services, including content and ads, to measure performance, and to communicate with users.<sup>42</sup>
- d. **Chrome Privacy Notice (“CPN”)**: The CPN describes features that are specific to Chrome, including the five browser modes: Basic browser mode, Sign-in mode, Sync mode, Incognito mode, and Guest mode. The CPN explains that “[y]ou can limit the information Chrome stores *on your system* by using incognito mode.” (emphasis added). It also explains that “Chrome won’t share existing cookies with sites you visit in incognito [...] mode. Sites may deposit new cookies on your system while you are in these modes, but they’ll only be stored and transmitted until you close the last incognito [...] window.”<sup>43</sup>

---

<sup>41</sup> I am informed that the version of the page that is linked to “Learn More” on the Incognito Splash Screen has changed over time. I understand from Counsel that the page titled, “How Private Browsing Works in Chrome” was linked to the version of the Incognito Splash Screen presented in the TAC for the majority of the Class Period. I am further informed that the versions of this page as of May 26, 2020 for desktop and July 6, 2020 for mobile are relevant for my report. “How Private Browsing Works in Chrome” (Desktop), May 26, 2020, *Google*, available at <https://web.archive.org/web/20200526023242/https://support.google.com/chrome/answer/7440301>; “How Private Browsing Works in Chrome” (Mobile), July 6, 2020, *Google*, available at <https://web.archive.org/web/20200706003245/https://support.google.com/chrome/answer/7440301?co=GENIE.Platform%3DiOS&oco=1>. See also, **Appendix I.1**.

<sup>42</sup> I am informed that the version of the PP as of March 31, 2020 is relevant for my report. “Google Privacy Policy,” March 31, 2020, *Google*, available at <https://policies.google.com/privacy/archive/20200331?hl=en-US>. See also, **Appendices M.1 and M.2**.

<sup>43</sup> I am informed that the version of the CPN as of May 20, 2020 is relevant for my report. “Chrome Privacy Notice,” May 20, 2020, *Google*, available at <https://www.google.com/chrome/privacy/archive/20200520/>. See also, **Appendices N.1 and N.2**.

CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

- e. ***New Account Creation Agreement.*** I understand that, in or around May 2018, Google revised the disclosures on its new account creation screen (the “New Account Creation Agreement”) to state that, “To create a Google Account, you’ll need to agree to the Terms of Service below. In addition, when you create an account, we process your information as described in our Privacy Policy, including these key points [...]”<sup>44</sup> The New Account Creation Agreement goes on to explain, among other things: “When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity – including information like the video you watched, device IDs, IP addresses, cookie data, and location. We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.”<sup>45</sup> The New Account Creation Agreement explains that Google uses the data to, among other things, “[d]eliver personalized ads, depending on your account settings, both on Google services and on sites and apps that partner with Google.”<sup>46</sup>
- f. ***Consent Bump Agreement.*** I understand that, in or around June 2016, Google pushed a new consent screen out to existing Google Account holders. I am informed that this screen is referred to as the “Consent Bump Agreement.”<sup>47</sup> The Consent Bump Agreement describes the types of user-generated data that may be stored in a user’s Account with his or her consent, and contains a MORE OPTIONS button that, when selected, offered the user to learn “More about these features.” Users who chose to learn “More about these features” were taken to a FAQ page that explains “What do we mean by ‘websites and apps that partner with Google?’” The page explains:

Many websites and apps use Google technologies to improve their content and services. For example, a website might use our

---

<sup>44</sup> Screenshot of New Account Creation Agreement Desktop, accessed on September 24, 2021. The screenshots of the New Account Creation Agreement I use in my report were taken on September 24, 2021 for desktop and September 30, 2021 for mobile. *See also*, **Appendix O**.

<sup>45</sup> Screenshot of New Account Creation Agreement Desktop, accessed on September 24, 2021. *See also*, **Appendix O**.

<sup>46</sup> Screenshot of New Account Creation Agreement Desktop, accessed on September 24, 2021. *See also*, **Appendix O**.

<sup>47</sup> I am informed that the version of the Consent Bump Agreement shown in a Google internal presentation dated August 2, 2016 (updated January 19, 2017) is also relevant for my report. GOOG-CABR-04067825-7867. *See also*, **Appendix P**.

advertising services (like AdSense) or analytics tools (like partners who use Google Analytics to improve the ads they show).

As you use these sites, your web browser may send certain information to Google that may include the web address of the page that you're visiting, your IP address, or cookies previously set by the site or Google. In the case of mobile apps, this could also include the name of the app and an identifier that helps us to determine which ads we've served to other apps on your device.

These features described today [*i.e.*, in the Consent Bump Agreement] don't change the types of data collected from these websites and apps – they simply change how that data is stored and used.<sup>48</sup>

## V. CONSUMER PREFERENCES FOR BROWSERS AND BROWSER FEATURES VARY, AND CONSUMER PERCEPTIONS AND EXPECTATIONS OF PRIVACY ARE CONTEXT SPECIFIC

### A. Consumer Preferences of Browsers and Browser Features Vary

42. Despite offering similar design features, settings, and tools, browsers differentiate themselves with various features that differ relative to other browsers in certain areas. For instance, according to a 2021 article published in PCMag, Chrome was rated better than other browsers on compatibility and speed on Windows operating systems, while Safari tested fastest on the MacOS. Opera is the only browser offering a built-in virtual private network (“VPN”). Edge offers voice-reading of webpages with realistic speech and Firefox incorporates an application called “Pocket,” which allows users to store certain content for easy access.<sup>49</sup> Most browsers offer a private browsing mode.<sup>50</sup> As all the major browsers are free to the public, inherent features such as ease of use and speed play a role in consumer choice.<sup>51</sup>
43. Consumers’ revealed preference across browsers and certain browser features can be inferred from the market share data. Chrome has the largest market share in the US since

---

<sup>48</sup> GOOG-CABR-04067825-7867. *See also*, **Appendix P**.

<sup>49</sup> Muchmore, Michael, “Chrome, Edge, Firefox, Opera, or Safari: Which Browser is Best?” May 20, 2021, *PCMag*, available at <<https://www.pcmag.com/picks/chrome-edge-firefox-opera-or-safari-which-browser-is-best>>, accessed on March 18, 2022.

<sup>50</sup> Klein, Matt, “How to Enable Private Browsing on Any Web Browser,” July 5, 2017, *How-To Geek*, available at: <<https://www.howtogeek.com/269265/how-to-enable-private-browsing-on-any-web-browser/#:~:text=To%20open%20a%20new%20InPrivate,return%20to%20regular%20browsing%20mode>>, accessed on April 5, 2022; C., Suresh, “How to Start Secret Mode and Add New Tab in Samsung Internet?,” March 17, 2022, *BrowserHow*, available at: <<https://browserhow.com/how-to-start-secret-mode-and-add-new-tab-in-samsung-internet/>>, accessed on April 5, 2022.

<sup>51</sup> Over half of respondents in a 2012 survey said ease of use and speed were important features, while only 13 percent didn't care about any particular feature and use the browser installed on their computer. *See* Pilon, Anne, “Web Browser Survey: Firefox Still Ahead of Chrome,” January 6, 2012, *AYTM*, available at <<https://aytm.com/blog/web-browser-survey/>>, accessed on March 18, 2022.

2014 and globally since 2013.<sup>52</sup> Market share data also shows that consumer preferences differ by device. As of 2022, the top browsers in US desktop market are Chrome (60%), Safari (18%), Edge (12%), and Firefox (6%).<sup>53</sup> During the same time, the top browsers in US mobile market are Safari (54%), Chrome (40%), and Samsung Internet (4%).<sup>54</sup> Although pre-installed browsers may have a unique advantage, they are not guaranteed market share. For example, Safari comes pre-installed as the default browser on Apple products, and Edge (and before that, Internet Explorer) comes pre-installed as the default browser on desktops with Windows operating systems. Safari benefits from the widespread use of the iPhone leading to its dominance on mobile devices. However, Microsoft's pre-installed browser is no longer the most used browser, despite Windows consistently dominating the desktop market for over a decade.<sup>55</sup> This illustrates that consumers' preferences of browser features (aside from what comes "pre-installed") play a role in their browser choice.

44. Additionally, it is common that consumers use multiple browsers. Indeed, as evidenced in the surveys I conducted for this case, more than half of respondents said that they used more than one browser.<sup>56</sup> Further, my survey data shows that mobile users indicated using Safari more than desktop users, which is consistent with trends observed in the public data.<sup>57</sup>

---

<sup>52</sup> Chrome has gained market share in the US every year since 2009 except for 2019 and 2020. Chrome's 2022 market has the highest current US market share with approximately 49 percent, exceeding the next closest competitor in Safari by over 12 percent. Chrome's global market share is even higher with approximately 63 percent in 2022. *See* "Browser Market Share United States of America, 2009-2022," *StatCounter*, available at <<https://gs.statcounter.com/browser-market-share/all/united-states-of-america/#yearly-2009-2022>>, accessed on March 18, 2022; *See also*, "Browser Market Share Worldwide," *StatCounter*, available at <<https://gs.statcounter.com/browser-market-share/#yearly-2009-2022>>, accessed on March 18, 2022.

<sup>53</sup> "Desktop Browser Market Share United States of America, 2016-2022," *StatCounter*, available at <<https://gs.statcounter.com/browser-market-share/desktop/united-states-of-america/#yearly-2016-2022>>, accessed on March 18, 2022.

<sup>54</sup> "Mobile Browser Market Share United States of America, 2016-2022," *StatCounter*, available at <<https://gs.statcounter.com/browser-market-share/mobile/united-states-of-america/#yearly-2016-2022>>, accessed on March 18, 2022.

<sup>55</sup> "Desktop Operating System Market Share Worldwide, 2009-2022," *StatCounter*, available at <<https://gs.statcounter.com/os-market-share/desktop/worldwide/#yearly-2009-2022>>, accessed on March 18, 2022; *See also*, "Desktop Browser Market Share Worldwide, 2009-2022," *StatCounter*, available at <<https://gs.statcounter.com/browser-market-share/desktop/worldwide/#yearly-2009-2022>>, accessed on March 18, 2022.

<sup>56</sup> Statistics are calculated using anyone that answered the question across all surveys.

<sup>57</sup> Statistics are calculated using anyone that answered the question across all surveys.

**B. Consumers' Concerns About Privacy Depend on The Context**

45. Consumers' concerns about privacy depend on the context and scenario, such as *which* people or entities have access to consumer information, *what* types of consumer information people or entities have access to, and *how* people or entities use this consumer information.<sup>58</sup> By giving up some level of privacy, consumers may receive benefits such as convenience and better access to services offered by websites.<sup>59</sup> For example, consumers may want to receive better, contextually relevant suggestions, so they willingly log-in to their Google Accounts and turn on their Web & App Activity, which results in their searches being stored in their Google Accounts.<sup>60</sup> Trade-offs and decisions regarding convenience and privacy vary greatly from one consumer to another.<sup>61</sup> As a result of context-specific privacy concerns and varying preferences, consumers' stated preferences do not always line up with their revealed preferences regarding privacy. This inconsistency, commonly referred to in the literature as the "privacy paradox," has been widely studied.<sup>62</sup>
46. To tailor services and products to meet the needs of consumers, companies traditionally use market segmentation,<sup>63</sup> with the ultimate form being direct marketing. As explained in

---

<sup>58</sup> For instance, consumers are less concerned about tech companies than hackers accessing one's data, less concerned about zip codes being accessed than health or financial data, and less concerned about the use of their data for the purpose of public safety than if it was used as a result of one's identity being stolen. GOOG-CABR-05156497-6555, at 6508-6510. As another example, in one study, a majority of respondents agreed that it was acceptable for employers to install monitoring cameras after multiple workplace thefts, while in another, a majority of respondents said they would not want a "smart thermostat" that tracked their movements inside their house installed in exchange for energy bill savings. Raine, Lee and Maeve Duggan, "Privacy and Information Sharing," January 14, 2016, *Pew Research Center*, available at <<https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/>>, accessed on April 5, 2022.

<sup>59</sup> See Oppmann, Patrick, "In Digital World, We Trade Privacy for Convenience," April 14, 2010, *CNN*, available at <<http://www.cnn.com/2010/TECH/04/14/oppmann.off.the.grid/index.html>>, accessed on March 29, 2022; Raine, Lee and Maeve Duggan, "Privacy and Information Sharing," January 14, 2016, *Pew Research Center*, available at <<https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/>>, accessed on April 5, 2022.

<sup>60</sup> See "Find & Control Your Web & App Activity," *Google*, available at <<https://support.google.com/websearch/answer/54068?hl=en&co=GENIE.Platform%3DDesktop>>, accessed on March 29, 2022.

<sup>61</sup> See for example, a study on smart speaker consumers and non-consumers found that for consumers who decided to purchase smart speakers, "the most prevalent motivating factor for purchasing a smart speaker was the convenience offered by smart speakers" while for non-consumers "other factors outweighed potential convenience." Lau, Josephine, et al., "Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers," *Proceedings of the ACM on Human-Computer Interaction*, Vol. 2, Issue CSCW, 2018, pp. 1-31, p. 9.

<sup>62</sup> See for example, Acquisti, Alessandro and Jens Grossklags, "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy*, Vol. 3, No. 1, 2005, pp. 26-33, pp. 27-29; See also, Athey, Susan, et al., "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk," *NBER Working Paper Series*, 2017, pp. 1-26, pp. 2,11-12.

<sup>63</sup> For example, as explained in *Principles of Marketing*, "Samsung successfully tailors emails—their design, messages, and offers—to the characteristics and needs of specific customers. Through its huge database, Samsung can send tailored messages to customers who just purchased a Samsung device or to people who are likely to purchase a Samsung device in the near future." This benefits Samsung by helping them build better relationships

CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

*Principles of Marketing*, “[b]ecause of the one-to-one nature of direct marketing, companies can [...] learn more about [customers’] needs, and personalize products and services to specific customer tastes.”<sup>64</sup> For example, retailers may use consumers’ transaction data to target coupons to specific consumers.<sup>65</sup> By allowing retailers to record their transaction histories, consumers may receive better promotions in exchange.

47. Consumers’ preferences over personalized ads also vary. One study finds that the majority of consumers prefer personalized ads over non-personalized ads due to the reduction of irrelevant ads, discovery of new products, and improved efficiency of searching and shopping.<sup>66</sup> Plaintiff Brown appears to hold the same preferences.<sup>67</sup> Another study on consumer interactions with Facebook’s personalized ads and privacy controls found that enhanced privacy controls increased consumer engagement with personalized ads, specifically for ads that used more unique information and for groups that were more likely to use opt-out privacy settings.<sup>68</sup>
48. As discussed in this section, consumer preferences vary when it comes to internet browsers and browser features, and consumers’ concerns about privacy vary depending on context. Therefore, to evaluate consumer understanding, perceptions, and expectations specific to the facts of this matter, and to evaluate whether and to what extent consumers’ understanding, perceptions, and expectations affect their likelihood of using a specific internet browser or browser feature, one needs to perform an empirical analysis using data and context relevant to this matter—in other words, this is what we call an empirical question. The importance of conducting empirical analysis is a topic I discussed

---

with their customers, and customers who are provided with the information most relevant to them. Kotler, Philip and Gary Armstrong, *Principles of Marketing*, Seventeenth Edition, Pearson, 2018 (“Kotler and Armstrong (2018)”), pp. 74-75, 511-515.

<sup>64</sup> Kotler and Armstrong (2018), p. 514.

<sup>65</sup> See Khan, Romana, et al., “Dynamic Customer Management and the Value of One-to-One Marketing,” *Marketing Science*, Vol. 28, No. 6, 2009, pp. 1063-1079, pp. 1064, 1072-1075, and 1077.

<sup>66</sup> Pauzer, Holly, “71% of Consumers Prefer Personalized Ads,” *Adlucent*, available at <<https://www.adlucent.com/resources/blog/71-of-consumers-prefer-personalized-ads/>>, accessed on April 14, 2022.

<sup>67</sup> “[I]n general, I think targeted advertising is a good thing.” See Brown Deposition, at 158:8-9. See also, Brown Deposition, at 82:7-8.

<sup>68</sup> Tucker, Catherine E., “Social Networks, Personalized Advertising, and Privacy Controls,” *Journal of Marketing Research*, Vol. LI, 2014, pp. 546-562.



extensively in a paper that I co-authored.<sup>69</sup> I designed and conducted my Consumer Perceptions and Expectations Study, Interpretation Study, and Likelihood of Use Study while considering the facts and allegations relevant to my assignment. I discuss these studies below in **Section VI** through **Section VIII**.

## VI. CONSUMER PERCEPTIONS AND EXPECTATIONS STUDY

49. Plaintiffs state that “[i]t is common knowledge that Google collects information about the web-browsing activity of users who are not in ‘private browsing mode’” and that “[i]t is also common knowledge that Google causes targeted advertisements to be sent based on that information.”<sup>70</sup> Plaintiffs affirmed this belief at their depositions.<sup>71</sup>
50. Nevertheless, Plaintiffs allege that “[b]ased on Google’s representations, Plaintiffs and Class members reasonably believed that their data would not be collected by Google and that Google would not intercept their communications when they were in ‘private browsing mode.’”<sup>72</sup> Specifically, Plaintiffs allege that “throughout the Class Period, Plaintiffs and Class members reasonably expected that Google would not collect their data while in Incognito mode.”<sup>73</sup>
51. In accordance with my assignment, I designed a Consumer Perceptions and Expectations Survey to assess users’ perceptions and expectations of the different types of entities that receive or not receive the At-Issue Data (such as IP address, URLs of the sites users visit, and cookies) when they visit websites while in private browsing mode. Users’ perceptions and expectations were assessed after viewing the private browsing splash screens for Chrome, Safari, or Firefox, as well as the “Learn More” pages that are linked to the Chrome and Firefox private browsing splash screens.

---

<sup>69</sup> Morales, Andrea C., et al., “Keeping it Real in Experimental Research —Understanding When, Where, and How to Enhance Realism and Measure Consumer Behavior,” *Journal of Consumer Research*, Vol. 44, No. 2, 2017, pp. 465-476, pp. 473-474.

<sup>70</sup> TAC, ¶ 163.

<sup>71</sup> See **Section IV.A** and footnote 16.

<sup>72</sup> TAC, ¶ 3.

<sup>73</sup> TAC, ¶ 53.

A. Study Design

52. Respondents were assigned to the Chrome group, Safari group, or Firefox group based on which internet browser(s) they stated that they currently used in response to one of the screening questions.<sup>74</sup> Respondents were presented with the private browsing splash screens for Chrome, Safari, or Firefox, as well as the “Learn More” pages that are linked to the Chrome (for those in the Chrome group) and Firefox private browsing splash screens (for those in the Firefox group), which contain additional information about private browsing.<sup>75</sup> (See **Table 1**.)

**Table 1. Consumer Perceptions and Expectations Survey Groups**

Chrome	Safari	Firefox
<ul style="list-style-type: none"><li>• Chrome Incognito Splash Screen</li><li>• “Learn More” page</li></ul>	<ul style="list-style-type: none"><li>• Safari Private Browsing Splash Screen</li></ul>	<ul style="list-style-type: none"><li>• Firefox Private Browsing Splash Screen</li><li>• “Learn More” page</li></ul>

53. After being presented with the private browsing splash screen (and “Learn More” page for Chrome and for Firefox), respondents were asked to express their understanding of whether and to what extent the three enumerated entities receive or do not receive data (such as IP address, URLs of the sites visited, and cookies) when they visit websites while in private browsing mode. The types of entities were companies that provide analytics and advertising services to websites visited, internet service providers, or companies that own the websites visited. Respondents chose from a scale of 1 = the type of entity does not receive the data from their private browsing session, 2 = the type of entity probably does not receive the data from their private browsing session, 3 = it is uncertain whether the type of entity receives the data from their private browsing session or not, 4 = the type of entity probably receives the data from their private browsing session, 5 = the type of entity does receive the data from their private browsing session. To avoid order effects, I randomized the order of the scale items to be either 1-2-3-4-5 or 5-4-3-2-1.<sup>76</sup> The respondent was

<sup>74</sup> QS7, “Thinking about the device(s) you use to browse the internet (such as your phone, your personal laptop, or your office computer), which internet browser(s) do you currently use? (*Select all that apply*).” **Appendix F.1**.

<sup>75</sup> There is no hyperlink on the Safari Private Browsing Splash Screen. Therefore, respondents who were presented with the Safari Private Browsing Splash Screen were not presented with the “Learn More” page.  
To simulate an organic browsing experience, the Chrome Incognito Splash Screen and the Firefox Private Browsing Splash Screen contained an active hyperlink that could be clicked to open the “Learn More” page. If respondents did not click on the hyperlink, they were still presented with the “Learn More” page after they were presented with the splash screen.

<sup>76</sup> Diamond (2011), pp. 395-396.



CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

presented with the same order of scale items across scale questions. Additionally, I randomized the order of the key questions to further mitigate order effects. For example, one respondent might have seen the question on companies that provide analytics and advertising to websites visited first, while another respondent might have seen the question on internet service providers first.<sup>77</sup>

54. If a large proportion of respondents chooses a value of 5, it would mean that, overall, respondents expect that the type of entity *does* receive the data from their private browsing session. If a large proportion of respondents chooses a value of 1, it would mean that, overall, respondents expect that the type of entity *does not* receive the data from their private browsing session.
55. The target population consists of adults residing in the US who use a private browsing mode. The number of targeted respondents is 500, with a minimum requirement of 200 respondents who were presented with the Chrome Incognito Splash Screen, a minimum requirement of 50 respondents who were presented with the Safari Private Browsing Splash Screen, and a minimum requirement of 50 respondents who were presented with the Firefox Private Browsing Splash Screen.

## B. Analysis and Results

56. **Tables 2 and 3** present results from the Consumer Perceptions and Expectations Survey. Results show that, overall, respondents expect that companies that provide analytics and advertising services to websites visited, internet service providers, and companies that own the websites visited *receive* data from their private browsing session (such as IP address, URLs of the sites visited, and cookies).<sup>78</sup> Around half of the respondents in the Chrome group (44% to 53%) expect that companies that provide analytics and advertising services to websites visited, internet service providers, and companies that own the websites visited *probably* or *do* receive (4 or 5 on the scale) the data from their private browsing session.
57. Only 15% to 20% of respondents in the Chrome group expect that companies that provide analytics and advertising services to websites visited, internet service providers, and companies that own the websites visited *do not* receive (1 on the scale) the data from their

---

<sup>77</sup> My survey instrument is available in **Appendix F.1**.

<sup>78</sup> My results are robust to different sensitivity analyses. For example, I cut the sample by age group, gender, and region and the findings from my results still hold.

CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

private browsing session. Even including respondents who answered *probably do not* receive, 26% to 35% of respondents in the Chrome group expect that entities *do not* or *probably do not* receive (1 or 2 on the scale) the data from their private browsing session. Results are similar when analyzing responses from respondents across all three internet browsers.

58. These findings are not consistent with Plaintiffs’ claim that “Class members reasonably believed that their data would not be collected by Google and that Google would not intercept their communications when they were in ‘private browsing mode.’”<sup>79</sup>

**Table 2. User Expectations of Certain Types of Entities  
Receiving Data from Their Private Browsing Session  
Distribution by Browser Presented**

“While in [MODE NAME] mode, does [TYPE OF ENTITY] receive or not receive the data from your [MODE NAME] session (such as IP address, URLs of the sites you visit, and cookies)?”

(1 = “[TYPE OF ENTITY] does not receive the data from my [MODE NAME] session,”  
2 = “[TYPE OF ENTITY] probably does not receive the data from my [MODE NAME] session,”  
3 = “It is uncertain whether [TYPE OF ENTITY] receives the data from my [MODE NAME] session or not,”  
4 = “[TYPE OF ENTITY] probably receives the data from my [MODE NAME] session,”  
5 = “[TYPE OF ENTITY] does receive the data from my [MODE NAME] session”)

	Chrome n=270		Safari n=135		Firefox n=126		All Respondents n=531	
	#	%	#	%	#	%	#	%
Companies that provide analytics and advertising services to websites you visited								
Do not (1)	55	20%	30	22%	29	23%	114	21%
Probably do not (2)	40	15%	21	16%	12	10%	73	14%
Uncertain (3)	37	14%	30	22%	14	11%	81	15%
Probably (4)	63	23%	26	19%	31	25%	120	23%
Do (5)	57	21%	11	8%	31	25%	99	19%
I don’t feel I have enough information to answer this question	18	7%	17	13%	9	7%	44	8%
Internet service provider								
Does not (1)	42	16%	30	22%	18	14%	90	17%
Probably does not (2)	29	11%	25	19%	14	11%	68	13%
Uncertain (3)	44	16%	31	23%	14	11%	89	17%
Probably (4)	63	23%	28	21%	30	24%	121	23%
Does (5)	80	30%	13	10%	43	34%	136	26%
I don’t feel I have enough information to answer this question	12	4%	8	6%	7	6%	27	5%
Companies that own the websites you visited								
Do not (1)	40	15%	25	19%	24	19%	89	17%
Probably do not (2)	35	13%	24	18%	16	13%	75	14%
Uncertain (3)	41	15%	22	16%	16	13%	79	15%
Probably (4)	66	24%	32	24%	24	19%	122	23%
Do (5)	67	25%	12	9%	37	29%	116	22%
I don’t feel I have enough information to answer this question	21	8%	20	15%	9	7%	50	9%

Source: Exhibits 3.1, 3.2, and 3.3.

<sup>79</sup> TAC, ¶ 3.

**Table 3. User Expectations of Certain Types of Entities  
Receiving Data from Their Private Browsing Session  
Proportions of “Low” Responses vs. Proportions of “High” Responses**

“While in [MODE NAME] mode, does [TYPE OF ENTITY] receive or not receive the data from your [MODE NAME] session (such as IP address, URLs of the sites you visit, and cookies)?”

- (1 = “[TYPE OF ENTITY] does not receive the data from my [MODE NAME] session,”  
2 = “[TYPE OF ENTITY] probably does not receive the data from my [MODE NAME] session,”  
3 = “It is uncertain whether [TYPE OF ENTITY] receives the data from my [MODE NAME] session or not,”  
4 = “[TYPE OF ENTITY] probably receives the data from my [MODE NAME] session,”  
5 = “[TYPE OF ENTITY] does receive the data from my [MODE NAME] session”)

	Chrome n=270	All Respondents n=531
	%	%
Companies that provide analytics and advertising services to websites you visited		
Do not (1) or Probably do not (2)	35%	35%
Probably (4) or Do (5)	44%	41%
Internet service provider		
Do not (1) or Probably do not (2)	26%	30%
Probably (4) or Do (5)	53%	48%
Companies that own the websites you visited		
Do not (1) or Probably do not (2)	28%	31%
Probably (4) or Do (5)	49%	45%

Source: Exhibits 4.1 and 4.2.

59. Overall, respondents in the Chrome group (*i.e.*, those who were presented with the Chrome Incognito Splash Screen and “Learn More” page) expect that companies that provide analytics and advertising services to websites visited, internet service providers, and companies that own the websites visited receive the data from their private browsing session.<sup>80</sup>

- a. 21% of respondents in the Chrome group expect that companies that provide analytics and advertising services to websites visited *do* receive (5 on the scale) the data from their private browsing session, and including those who answered *probably* receive (4 or 5 on the scale), the proportion of respondents is close to half (44%). 20% of respondents in the Chrome group expect that companies that provide analytics and advertising services to websites visited *do not* receive (1 on the scale) the data from their private browsing session. Even including those who answered *probably do not* receive (1 or 2 on the scale), the proportion of respondents is 35%.

<sup>80</sup> For each type of entity, the proportion of respondents who answered *do not* receive (1 on the scale) is statistically significantly less than 30% (p<0.05 using the one-tailed, one sample equality test of proportions).

For each type of entity, the proportion of respondents who answered *do not* or *probably do not* receive (1 or 2 on the scale) is statistically significantly less than 50% (p<0.05 using the one-tailed, one sample equality test of proportions).

For each type of entity, the proportion of respondents who answered *do not* or *probably do not* receive (1 or 2 on the scale) is statistically significantly less than the proportion of respondents who answered *probably* or *do* receive (4 or 5 on the scale) (p<0.05 using the one-tailed, two sample equality test of proportions). **Tables 2 and 3 and Exhibits 3.1, 3.2, 3.3, 4.1, and 4.2.**

- b. 30% of respondents in the Chrome group expect that internet service providers *do* receive (5 on the scale) the data from their private browsing session, and including those who answered *probably* receive (4 or 5 on the scale), the proportion of respondents is over half (53%). Only 16% of respondents in the Chrome group expect that internet service providers *do not* receive (1 on the scale) the data from their private browsing session. Even including those who answered *probably do not* receive (1 or 2 on the scale), the proportion of respondents is 26%.
  - c. 25% of respondents in the Chrome group expect that companies that own the websites visited *do* receive (5 on the scale) the data from their private browsing session, and including those who answered *probably* receive (4 or 5 on the scale), the proportion of respondents is close to half (49%). Only 15% of respondents in the Chrome group expect that companies that own the websites visited *do not* receive (1 on the scale) the data from their private browsing session. Even including those who answered *probably do not* receive (1 or 2 on the scale), the proportion of respondents is 28%.
60. Results are consistent when analyzed across respondents in all three groups (*i.e.*, respondents who were presented with the Chrome Incognito Splash Screen and “Learn More” page, the Safari Private Browsing Splash Screen, or the Firefox Private Browsing Splash Screen and “Learn More” page).<sup>81</sup> 19% of all respondents expect that companies that provide analytics and advertising services to websites visited *do* receive (5 on the scale) the data from their private browsing session, and including those who answered *probably* receive (4 or 5 on the scale), the proportion of respondents is 41%. 21% of all respondents expect that companies that provide analytics and advertising services to websites visited *do not* receive (1 on the scale) the data from their private browsing session.

---

<sup>81</sup> For each type of entity, the proportion of respondents who answered *do not* receive (1 on the scale) is statistically significantly less than 30% ( $p < 0.05$  using the one-tailed, one sample equality test of proportions).

For each type of entity, the proportion of respondents who answered *do not* or *probably do not* receive (1 or 2 on the scale) is statistically significantly less than 50% ( $p < 0.05$  using the one-tailed, one sample equality test of proportions).

For each type of entity, the proportion of respondents who answered *do not* or *probably do not* receive (1 or 2 on the scale) is statistically significantly less than the proportion of respondents who answered *probably* or *do* receive (4 or 5 on the scale) ( $p < 0.05$  using the one-tailed, two sample equality test of proportions). **Tables 2 and 3 and Exhibits 3.1, 3.2, 3.3, 4.1, and 4.2.**

Even including those who answered *probably do not* receive (1 or 2 on the scale), the proportion of respondents is 35%.

## VII. INTERPRETATION STUDY

61. Plaintiffs all testified that they read Google's Privacy Policy.<sup>82</sup> They further state that "[i]t is common knowledge that Google collects information about the web-browsing activity of users who are not in 'private browsing mode'" and that "[i]t is also common knowledge that Google causes targeted advertisements to be sent based on that information."<sup>83</sup> Plaintiffs affirmed at their depositions that they understood Google collects the At-Issue Data when they are in a browsing mode other than private browsing mode.<sup>84</sup>
62. Plaintiffs also claim that "[n]othing in Google's Privacy Policy or Incognito Screen leads users to believe that during private browsing Google continues to persistently monitor them [...] In fact, when the Privacy Policy and Incognito Screen are read together, the user necessarily reaches the opposite conclusion."<sup>85</sup>
63. In accordance with my assignment, I designed an Interpretation Survey to determine whether and to what extent users expect Google to receive or to not receive URLs of the sites users visit, IP addresses, and cookies placed on users' browsers during their private browsing session after reviewing the Incognito Splash Screen and "Learn More" page, as well as the PP and CPN,<sup>86</sup> the New Account Creation Agreement, or the Consent Bump Agreement for some respondents.

### A. Study Design

64. Respondents were randomly assigned to one of four groups with different sets of screens and policies presented: "Splash Screen Only," "Splash Screen with Policies (Highlighted)," "Splash Screen with New Account Creation Agreement," and "Splash Screen with Consent Bump Agreement and FAQ Page." (See **Table 4.**)

---

<sup>82</sup> See Byatt Deposition, at 23:2-18, 29:5-20; Davis Deposition, at 48:19-49:6, 51:11-18, 93:13-21; Trujillo Deposition, at 36:2-12; Brown Deposition, at 30:19-31:1, 33:2-4; Castillo Deposition, at 24:18-25:20.

<sup>83</sup> TAC, ¶ 163.

<sup>84</sup> See **Section IV.A** and footnote 16.

<sup>85</sup> TAC, ¶ 57.

<sup>86</sup> The Complaint alleges that the CPN, the PP, and the Incognito Splash Screen are part of the contract between Google and Class members. TAC, ¶ 268.

65. All respondents were presented with the Chrome Incognito Splash Screen as well as the “Learn More” page that is linked to the Incognito Splash Screen, which contains additional information about private browsing.<sup>87</sup> Based on which group they were assigned to, respondents were also shown either no additional documents (Splash Screen Only group), the PP and CPN (with and without highlights drawing attention to language relevant to Plaintiffs’ allegations) (Splash Screen with Policies (Highlighted) group),<sup>88</sup> the New Account Creation Agreement (Splash Screen with New Account Creation Agreement group), or the Consent Bump Agreement and FAQ Page (Splash Screen with Consent Bump Agreement and FAQ Page).

Table 4. Interpretation Survey Groups

<b>Splash Screen Only</b>	<ul style="list-style-type: none"><li>• Incognito Splash Screen</li><li>• “Learn More” page</li></ul>
<b>Splash Screen with Policies (Highlighted)</b>	<ul style="list-style-type: none"><li>• Google Privacy Policy, March 31, 2020 (with and without highlights)</li><li>• Chrome Privacy Notice, May 20, 2020 (with and without highlights)</li><li>• Incognito Splash Screen</li><li>• “Learn More” page</li></ul>
<b>Splash Screen with New Account Creation Agreement</b>	<ul style="list-style-type: none"><li>• New Account Creation Agreement</li><li>• Incognito Splash Screen</li><li>• “Learn More” page</li></ul>
<b>Splash Screen with Consent Bump Agreement and FAQ Page</b>	<ul style="list-style-type: none"><li>• Consent Bump Agreement and FAQ page</li><li>• Incognito Splash Screen</li><li>• “Learn More” page</li></ul>

66. After reviewing the Incognito Splash Screen, “Learn More” screen, and any assigned policies, each respondent was asked a series of three scale questions. These questions required respondents to express their understanding of whether Google receives or does not receive three types of data while in Incognito mode: URLs of the sites visited, IP addresses, and cookies placed on the browser. Respondents chose from a scale of 1 = Google does not receive this information, 2 = Google probably does not receive this

<sup>87</sup> In the same manner as in the Consumer Perceptions and Expectations Study, to simulate an organic browsing experience, the Incognito Splash Screen contained an active hyperlink that could be clicked to open the “Learn More” page. If respondents did not click on the hyperlink, they were still presented with the “Learn More” page after they were presented with the Incognito Splash Screen.

<sup>88</sup> In order to draw attention to the language relevant to Plaintiffs’ allegations, “respondents could be shown only the disputed text; or, as the realists advocate, they could be exposed to additional facts surrounding the case.” Since the survey method “rel[ies] on respondents with limited attention and sophistication” it should “restrict[] the quantum of such background facts.” Ben-Shahar and Strahilevitz (2017), p. 1778.



information, 3 = It is uncertain whether Google receives this information or not, 4 = Google probably receives this information, 5 = Google does receive this information.<sup>89, 90</sup>

67. If a large proportion of respondents chooses a value of 5, it would mean that, overall, respondents expect that Google *does* receive the specific types of data while in Incognito mode. If a large proportion of respondents chooses a value of 1, it would mean that, overall, respondents expect that Google *does not* receive the specific types of data while in Incognito mode.
68. The target population consisted of adults residing in the US who use private browsing mode. The number of targeted respondents is 1,000, with a target of 250 respondents in each group.

## B. Analysis and Results

69. **Tables 5 and 6** present results from the Interpretation Survey. Results show that, overall, respondents expect that Google receives URLs of the sites visited, IP addresses, and cookies placed on the browser while in Incognito mode.<sup>91,92</sup> Over half of the respondents in each group (52% to 55%) expect that Google *probably* receives or *does* receive (4 or 5 on the scale) URLs of the sites visited while in Incognito mode, over half of respondents in each group (62% to 65%) expect that Google *probably* receives or *does* receive (4 or 5 on the scale) IP addresses while in Incognito mode, and close to half of respondents in each group (46% to 55%) expect that Google *probably* receives or *does* receive (4 or 5 on the scale) cookies placed on the browser while in Incognito mode.
70. In each group, 13% to 19% of respondents expect that Google *does not* receive (1 on the scale) URLs of the sites visited while in Incognito mode, 6% to 12% of respondents expect that Google *does not* receive (1 on the scale) IP addresses while in Incognito mode, and 17% to 25% of respondents expect that Google *does not* receive (1 on the scale) cookies

---

<sup>89</sup> Like in my other surveys, to avoid order effects, I randomized the order of the scale items to be either 1-2-3-4-5 or 5-4-3-2-1. The respondent was presented with the same order of scale items across scale questions. Additionally, I randomized the order of the key questions to further mitigate order effects. Diamond (2011), pp. 395-396.

<sup>90</sup> My survey instrument is available in **Appendix F.2**.

<sup>91</sup> Note that the survey responses indicates that users anticipate that Google receives information in private browsing mode generally, even though, in reality, they would only receive this information if the website uses Google's services.

<sup>92</sup> My results are robust to different sensitivity analyses. For example, I cut the sample by age group, gender, and region and the findings from my results still hold.

CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

placed on the browser while in Incognito mode. Even including respondents who answered *probably does not* receive, 25% to 29% respondents expect that Google *does not* or *probably does not* receive (1 or 2 on the scale) URLs of the sites visited while in Incognito mode. The percentage of respondents that expect that Google *does not* or *probably does not* receive (1 or 2 on the scale) IP addresses is 14% to 20% and for cookies placed on the browser is 29% to 38%.

71. These findings are not consistent with Plaintiffs' claim that "[n]othing in Google's Privacy Policy or Incognito Screen leads users to believe that during private browsing Google continues to persistently monitor them [...] In fact, when the Privacy Policy and Incognito Screen are read together, the user necessarily reaches the opposite conclusion."<sup>93</sup>

---

<sup>93</sup> TAC, ¶ 57.



CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

**Table 5. User Interpretation of Google Receiving Certain Types of Data  
from Their Incognito Session  
Distribution by Group**

*“Based on the screens that you reviewed, please select one of the following regarding [DATA TYPE] during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product): ”*

*(1 = “Google does not receive this information”  
2 = “Google probably does not receive this information,”  
3 = “It is uncertain whether Google receives this information or not,”  
4 = “Google probably receives this information”  
5 = “Google does receive this information”)*

	Splash Screen Only		Splash Screen with Policies (Highlighted)		Splash Screen with New Account Creation Agreement		Splash Screen with Consent Bump Agreement and FAQ Page	
	n=254		n=254		n=252		n=253	
	#	%	#	%	#	%	#	%
URLs of the sites you visit								
Does not (1)	33	13%	47	19%	35	14%	43	17%
Probably does not (2)	34	13%	22	9%	29	12%	31	12%
Uncertain (3)	35	14%	23	9%	31	12%	16	6%
Probably (4)	69	27%	52	20%	58	23%	77	30%
Does (5)	68	27%	87	34%	74	29%	62	25%
I don’t feel I have enough information to answer this question	15	6%	23	9%	25	10%	24	9%
IP address								
Does not (1)	14	6%	30	12%	20	8%	25	10%
Probably does not (2)	21	8%	19	7%	22	9%	25	10%
Uncertain (3)	28	11%	19	7%	30	12%	26	10%
Probably (4)	70	28%	68	27%	62	25%	75	30%
Does (5)	95	37%	92	36%	99	39%	81	32%
I don’t feel I have enough information to answer this question	26	10%	26	10%	19	8%	21	8%
Cookies placed on your browser								
Does not (1)	59	23%	53	21%	43	17%	64	25%
Probably does not (2)	37	15%	28	11%	31	12%	32	13%
Uncertain (3)	26	10%	10	4%	29	12%	15	6%
Probably (4)	60	24%	58	23%	55	22%	58	23%
Does (5)	57	22%	82	32%	68	27%	67	26%
I don’t feel I have enough information to answer this question	15	6%	23	9%	26	10%	17	7%

Source: Exhibits 7.1, 7.2, and 7.3.

**Table 6. User Interpretation of Google Receiving Certain Types of Data from Their Incognito Session**  
**Proportions of “Low” Responses vs. Proportions of “High” Responses**

“Based on the screens that you reviewed, please select one of the following regarding [DATA TYPE] during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product): ”

- (1 = “Google does not receive this information”  
2 = “Google probably does not receive this information,”  
3 = “It is uncertain whether Google receives this information or not,”  
4 = “Google probably receives this information”  
5 = “Google does receive this information”)

	Splash Screen Only	Splash Screen with Policies (Highlighted)	Splash Screen with New Account Creation Agreement	Splash Screen with Consent Bump Agreement and FAQ Page
	n=254	n=254	n=252	n=253
	%	%	%	%
URLs of the sites you visit				
Does not (1) or Probably does not (2)	26%	27%	25%	29%
Probably (4) or Does (5)	54%	55%	52%	55%
IP address				
Does not (1) or Probably does not (2)	14%	19%	17%	20%
Probably (4) or Does (5)	65%	63%	64%	62%
Cookies placed on your browser				
Does not (1) or Probably does not (2)	38%	32%	29%	38%
Probably (4) or Does (5)	46%	55%	49%	49%

Source: Exhibits 8.1 and 8.2.

72. Overall, respondents in the Splash Screen Only group expect that Google receives URLs of the sites visited, IP addresses, and cookies placed on the browser while in Incognito mode.<sup>94</sup>

- a. 27% of respondents in the Splash Screen Only group expect that Google *does* receive (5 on the scale) URLs of the sites visited while in Incognito mode, and including those who answered *probably* receives (4 or 5 on the scale), the proportion of respondents is over half (54%). Only 13% of respondents in the Splash Screen Only group expect that Google *does not* receive (1 on the scale) URLs of the sites visited while in Incognito mode. Even including those who answered *probably does not* receive (1 or 2 on the scale), the proportion of respondents is 26%.

<sup>94</sup> For each type of data, the proportion of respondents who answered *does not* receive (1 on the scale) is statistically significantly less than 30% (p<0.05 using the one-tailed, one sample equality test of proportions).  
For each type of data, the proportion of respondents who answered *does not* or *probably does not* receive (1 or 2 on the scale) is statistically significantly less than 50% (p<0.05 using the one-tailed, one sample equality test of proportions).  
For each type of data, the proportion of respondents who answered *does not* or *probably does not* receive (1 or 2 on the scale) is statistically significantly less than the proportion of respondents who answered *probably* receives or *does* receive (4 or 5 on the scale) (p<0.05 using the one-tailed, two sample equality test of proportions). **Tables 5 and 6 and Exhibits 7.1, 7.2, 7.3, 8.1, and 8.2.**

- b. 37% of respondents in the Splash Screen Only group expect that Google *does* receive (5 on the scale) IP addresses while in Incognito mode, and including those who answered *probably* receives (4 or 5 on the scale), the proportion of respondents is over half (65%). Only 6% of respondents in the Splash Screen Only group expect that Google *does not* receive (1 on the scale) IP addresses while in Incognito mode. Even including those who answered *probably does not* receive (1 or 2 on the scale), the proportion of respondents is 14%.
  - c. 22% of respondents in the Splash Screen Only group expect that Google *does* receive (5 on the scale) cookies placed on the browser while in Incognito mode, and including those who answered *probably* receives (4 or 5 on the scale), the proportion of respondents is close to half (46%). 23% of respondents in the Splash Screen Only group expect that Google *does not* receive (1 on the scale) cookies placed on the browser while in Incognito mode. Even including those who answered *probably does not* receive (1 or 2 on the scale), the proportion of respondents is 38%.
- 73. Results are consistent among respondents in the Splash Screen with Policies (Highlighted) group, Splash Screen with New Account Creation Agreement group, and Splash Screen with Consent Bump Agreement and FAQ Page group.<sup>95</sup>
  - a. Overall, respondents in these three groups expect that Google receives URLs of the sites visited while in Incognito mode. 25% to 34% of respondents in each of these three groups expect that Google *does* receive (5 on the scale) URLs of the sites visited while in Incognito mode, and including those who answered *probably* receives (4 or 5 on the scale), the proportions of respondents in each of these three groups are over half (52% to 55%). Only 14% to 19% of

---

<sup>95</sup> For each type of data, the proportion of respondents who answered *does not* receive (1 on the scale) is statistically significantly less than 30% ( $p < 0.05$  using the one-tailed, one sample equality test of proportions). The exception is the proportion of respondents who answered *does not* receive (1 on the scale) for cookies placed on the browser in the Splash Screen with Consent Bump Agreement and FAQ Page group, which is marginally significantly less than 30% ( $p < 0.1$ ).

For each type of data, the proportion of respondents who answered *does not* or *probably does not* receive (1 or 2 on the scale) is statistically significantly less than 50% ( $p < 0.05$  using the one-tailed, one sample equality test of proportions).

For each type of data, the proportion of respondents who answered *does not* or *probably does not* receive (1 or 2 on the scale) is statistically significantly less than the proportion of respondents who answered *probably* receives or *does* receive (4 or 5 on the scale) ( $p < 0.05$  using the one-tailed, two sample equality test of proportions). **Tables 5 and 6 and Exhibits 7.1, 7.2, 7.3, 8.1, and 8.2.**

CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

respondents in each of these three groups expect that Google *does not* receive (1 on the scale) URLs of the sites visited while in Incognito mode. Even including those who answered *probably does not* receive (1 or 2 on the scale), the proportions of respondents in each of these three groups are between 25% and 29%.

- b. Overall, respondents in these three groups expect that Google receives IP addresses while in Incognito mode. 32% to 39% of respondents in each of these three groups expect that Google *does* receive (5 on the scale) IP addresses while in Incognito mode, and including those who answered *probably* receives (4 or 5 on the scale), the proportions of respondents in each of these three groups are over half (62% to 64%). Only 8% to 12% of respondents in each of these three groups expect that Google *does not* receive (1 on the scale) IP addresses while in Incognito mode. Even including those who answered *probably does not* receive (1 or 2 on the scale), the proportions of respondents in each of these three groups are between 17% and 20%.
- c. Overall, respondents in these three groups expect that Google receives cookies placed on the browser while in Incognito mode. 26% to 32% of respondents in each of these three groups expect that Google *does* receive (5 on the scale) cookies placed on the browser while in Incognito mode, and including those who answered *probably* receives (4 or 5 on the scale), the proportions of respondents in each of these three groups is around half (49% to 55%). 17% to 25% of respondents in each of these three groups expect that Google *does not* receive (1 on the scale) cookies placed on the browser while in Incognito mode. Even including those who answered *probably does not* receive (1 or 2 on the scale), the proportions of respondents in each of these three groups are between 29% and 38%.

## VIII. LIKELIHOOD OF USE STUDY

- 74. Plaintiffs allege that Chrome users understood the text on Chrome's Incognito Splash Screen "to mean they could browse privately, without Google's continued tracking and

data collection.”<sup>96</sup> Additionally, Plaintiffs allege that “Google left the misleading impression that users’ data was not being intercepted and collected without their knowledge and omitted to disclose the ways in which Google actually intercepts and uses user data in private browsing sessions.”<sup>97</sup> Plaintiffs state that “Google could have disclosed on this Incognito Screen that Google would track users and collect their data while they were browsing privately, but Google did not do that.”<sup>98</sup> At the motion to dismiss stage, the Court noted that “the Incognito Splash Screen omits Google from the list of entities that can view a user’s activity in private browsing mode,” and “a reasonable user could have read the two phrases [(‘Now you can browse privately’ and ‘other people who use this device won’t see your activity’)] as being independent of each other.”<sup>99</sup>

75. In accordance with my assignment, I designed a Likelihood of Use Survey to determine whether and to what extent modification of certain language on the Incognito Splash Screen and the “Learn More” page that address Plaintiffs’ criticisms of those documents—namely, that these documents should have identified Google as an entity that may receive data when an Incognito user visits a website using Google services—impacts users’ likelihood to use Chrome in Incognito mode for private browsing.

#### A. Study Design

76. For this survey, I used a test/control experimental design. In such a design, respondents in two groups (test and control) are presented with different versions of the stimuli, and they answer the same set of questions. Having a control group can correct for any preexisting beliefs or other influences that would have produced similar response levels in both the test and control groups, therefore eliminating the effects of any background noise on results and isolating the causal effect of the hypothesized causal variable on a respondent’s response.<sup>100</sup> A comparison between the answers provided by respondents in these two groups creates the ability to evaluate the effect of different wording used in the two stimuli

---

<sup>96</sup> TAC, ¶ 53.

<sup>97</sup> TAC, ¶ 151.

<sup>98</sup> TAC, ¶ 53.

<sup>99</sup> Order Denying Motion to Dismiss, *Chasom Brown et al., Plaintiffs, v. Google LLC, Defendant*, United States District Court, Northern District of California – Oakland Division, No. 5:20-cv-03664-YGR, March 12, 2021, pp. 17-18.

<sup>100</sup> Diamond (2011), pp. 398-399.

and “assess[] responses to closed-ended questions.”<sup>101</sup> Therefore, “the focus on the response level in a control group design is not on the absolute response level, but on the difference between the response level of the experimental group and that of the control group.”<sup>102</sup>

77. Respondents in this study were randomly assigned to either the Actual Language group or the Alternative Language group. (See **Table 7.**)

**Table 7. Likelihood of Use Survey Experimental Groups**

Actual Language Group	Alternative Language Group
<ul style="list-style-type: none"><li>Actual Chrome Incognito Splash Screen</li><li><i>(If respondent clicked the “Learn more” hyperlink)</i> Actual “Learn More” page</li></ul>	<ul style="list-style-type: none"><li>Alternative Chrome Incognito Splash Screen</li><li><i>(If respondent clicked the “Learn more” hyperlink)</i> Alternative “Learn More” page</li></ul>

78. Because this survey is about users’ actual behavior and because context matters, I presented a scenario to simulate the browsing experience. This scenario was the same across all respondents. This scenario asked respondents to imagine that they were researching a sensitive topic online and they decided to browse the web in private browsing mode.

79. Following the presentation of the scenario, respondents that were assigned to the Actual Language group were presented with the actual Incognito Splash Screen. This screen contained an active hyperlink that could be clicked to open the “Learn More” screen. If respondents clicked on the hyperlink, they were also presented with the actual “Learn More” page that contains additional information about Incognito mode.

80. Respondents that were assigned to the Alternative Language group were presented with the same set of stimuli as those in the Actual Language group, except that certain language on the Incognito Splash Screen and on the “Learn More” page was modified. Specifically, in the alternative version of the Incognito Splash Screen, the introductory sentence, “Now you can browse privately, and other people who use this device won’t see your activity” was modified to say, “Now you can browse privately, which means other people who use this device won’t see your activity.” Similarly, under the heading, “Your activity might still be visible to,” I added a bullet that stated: “Companies that provide services to websites you visit (such as Google Analytics, Adobe Analytics, Google Ad Manager, Facebook

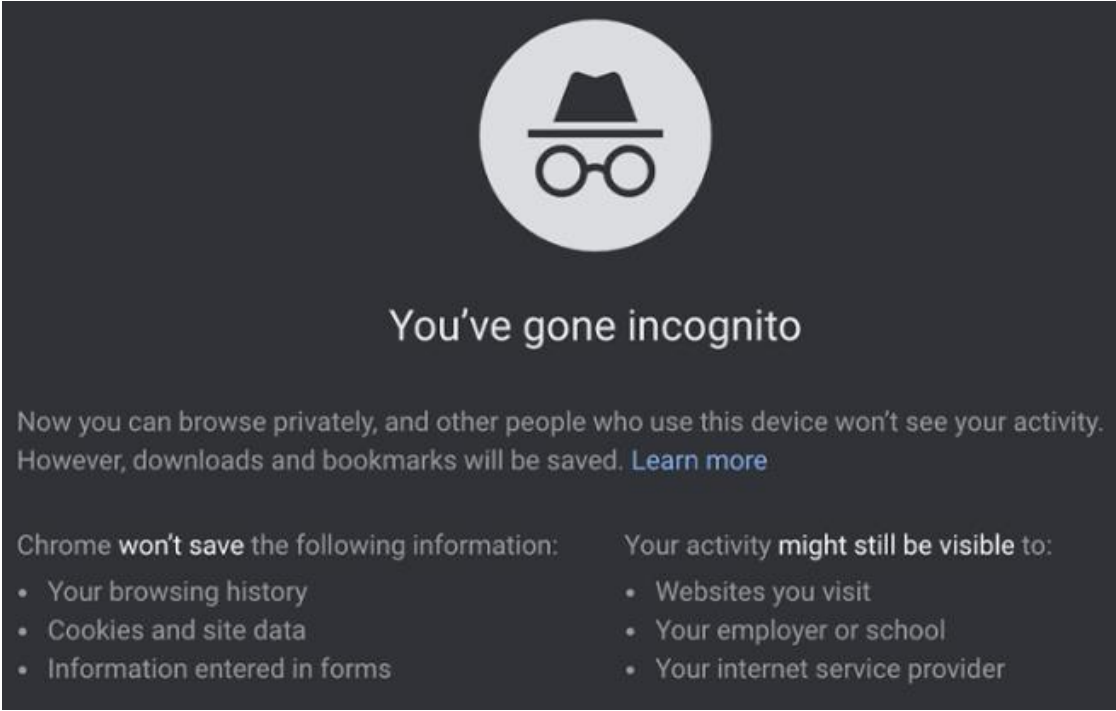
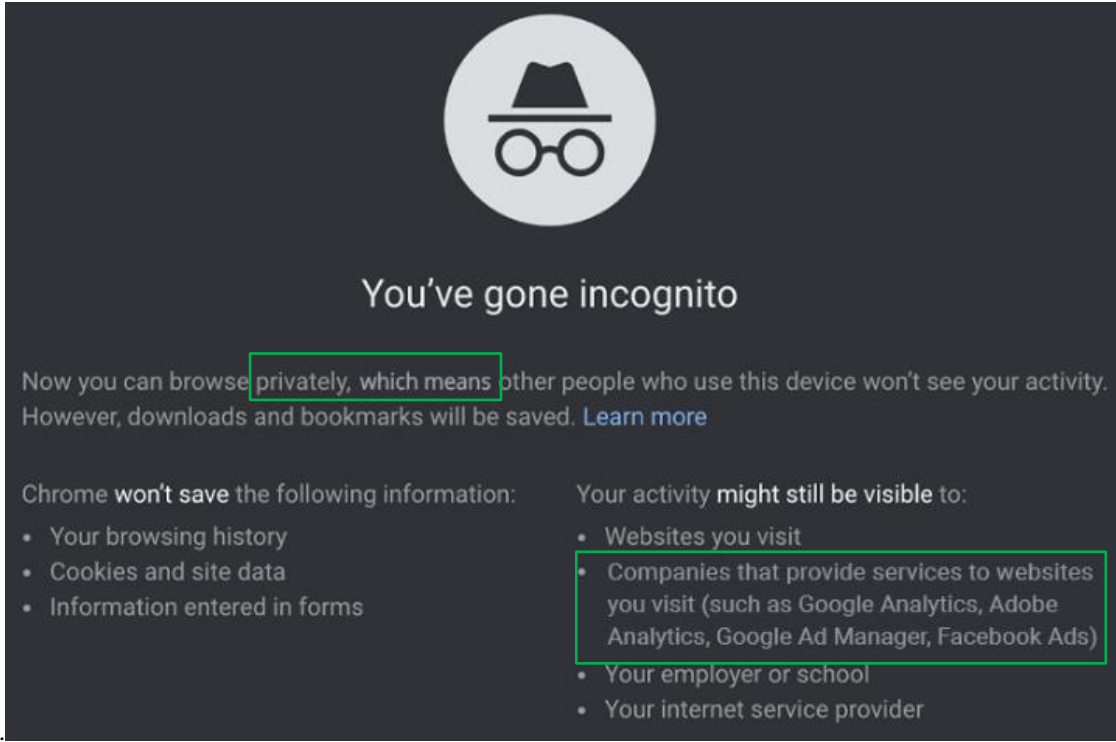
<sup>101</sup> Diamond (2011), p. 399.

<sup>102</sup> Diamond (2011), p. 399.

CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

Ads).” These language modifications address Plaintiffs’ allegations as to how the actual language in the Incognito Splash Screen allegedly is misleading. **Tables 8 and 9** below show the excerpts of the actual and alternative images presented to the respondents. The green textboxes indicate the location and edits made.<sup>103</sup>

**Table 8. Excerpts of Actual Language and Alternative Language (Incognito Splash Screen)**

Actual Incognito Splash Screen
 The image shows the standard Chrome Incognito splash screen. At the top is a circular icon with a hat and glasses. Below it, the text reads "You've gone incognito". A paragraph follows: "Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. <a href="#">Learn more</a> ". Below this, two columns of information are listed. The left column, titled "Chrome won't save the following information:", lists: "Your browsing history", "Cookies and site data", and "Information entered in forms". The right column, titled "Your activity might still be visible to:", lists: "Websites you visit", "Your employer or school", and "Your internet service provider".
Alternative Incognito Splash Screen
 This image is an alternative version of the Incognito splash screen. It features the same hat and glasses icon and "You've gone incognito" heading. The explanatory paragraph is identical, but the word "privately" is enclosed in a green rectangular box. The list of information not saved is the same. The list of where activity might be visible is also the same, but the item "Companies that provide services to websites you visit (such as Google Analytics, Adobe Analytics, Google Ad Manager, Facebook Ads)" is enclosed in a green rectangular box.

<sup>103</sup> See **Appendices H.1, H.2, I.1, and I.2** for the full images presented to the respondents.



Table 9. Excerpts of Actual Language and Alternative Language (“Learn More” Page)

Actual “Learn More” Page
<p><b>Your activity might still be visible</b></p> <p>Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:</p> <ul style="list-style-type: none"><li>• Websites you visit, including the ads and resources used on those sites</li><li>• Websites you sign in to</li><li>• Your employer, school, or whoever runs the network you’re using</li><li>• Your internet service provider</li><li>• Search engines<ul style="list-style-type: none"><li>• Search engines may show search suggestions based on your location or activity in your current Incognito browsing session.</li></ul></li></ul> <p><b>Some of your info might still be visible</b></p> <p>A web service, website, search engine, or provider may be able to see:</p> <ul style="list-style-type: none"><li>• Your IP address, which can be used to identify your general location</li><li>• Your activity when you use a web service</li><li>• Your identity if you sign in to a web service, like Gmail</li></ul> <p>You can still find and use your payment, password and contact info, but you can’t change your saved info in a Chrome Incognito window.</p>
Alternative “Learn More” Page
<p><b>Your activity might still be visible</b></p> <p>Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:</p> <div><ul style="list-style-type: none"><li>• Websites you visit, including the ads and resources used on those sites (such as Google Analytics, Adobe Analytics, Google Ad Manager, Facebook Ads)</li></ul></div> <ul style="list-style-type: none"><li>• Websites you sign in to</li><li>• Your employer, school, or whoever runs the network you’re using</li><li>• Your internet service provider</li><li>• Search engines<ul style="list-style-type: none"><li>• Search engines may show search suggestions based on your location or activity in your current Incognito browsing session.</li></ul></li></ul> <p><b>Some of your info might still be visible</b></p> <div><p>A web service (such as Google Analytics, Adobe Analytics, Google Ad Manager, Facebook Ads), website, search engine, or provider may be able to see:</p><ul style="list-style-type: none"><li>• Your IP address, which can be used to identify your general location</li><li>• Your activity when you use a web service</li><li>• Your identity if you sign in to a web service, like Gmail</li></ul></div> <p>You can still find and use your payment, password and contact info, but you can’t change your saved info in a Chrome Incognito window.</p>

81. After viewing the Incognito Splash Screen and for some respondents, the “Learn More” screen, respondents were asked how likely or unlikely they were to use the Chrome browser in Incognito mode to do online research on a sensitive topic. Respondents were asked to indicate the likelihood that they would use Chrome in Incognito mode to do online research on a sensitive topic on a scale of 1 (Unlikely) to 5 (Likely). Average likelihood of using Chrome in Incognito mode to do online research on a sensitive topic was calculated by

CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

using the numerical values associated with each response option (1 = Unlikely to use the Chrome browser in Incognito mode, 2 = Somewhat unlikely to use the Chrome browser in Incognito mode, 3 = Neither likely nor unlikely to use the Chrome browser in Incognito mode, 4 = Somewhat likely to use the Chrome browser in Incognito mode, and 5 = Likely to use the Chrome browser in Incognito mode).<sup>104, 105</sup> If the average value is close to 5, this means the average respondent will likely use Chrome in Incognito mode to do online research on a sensitive topic, whereas if the average value is close to 1, this means the average respondent will unlikely use Chrome in Incognito mode to do online research on a sensitive topic.

82. The target population consists of adults residing in the US who use a private browsing mode. The number of targeted respondents is 1,000, with a target of 500 respondents in each experimental group.

## B. Analysis and Results

83. **Figure 4 and Table 10** present my Likelihood of Use Survey results and show respondents' average likelihood of using Chrome for online research on a sensitive topic. Results show that the average respondent would likely use Chrome in Incognito mode to do online research on a sensitive topic after viewing the Incognito Splash Screen and for some respondents, the "Learn More" page. Importantly, modifying certain language on the Incognito Splash Screen and the "Learn More" page (*i.e.*, the second phrase in the introductory sentence and information regarding the list of entities to which users' activity might still be visible) to address Plaintiffs' criticisms regarding what those documents *should* disclose *has no statistically significant impact on respondents' likelihood of using Chrome in Incognito mode to do online research on a sensitive topic.*<sup>106</sup> This finding shows that including language that Plaintiffs claim "Google could have disclosed on [the] Incognito Screen [to describe] that Google would track users and collect their data while

---

<sup>104</sup> Like in my other surveys, to avoid order effects, I randomized the order of the scale items to be either 1-2-3-4-5 or 5-4-3-2-1. Diamond (2011), pp. 395-396.

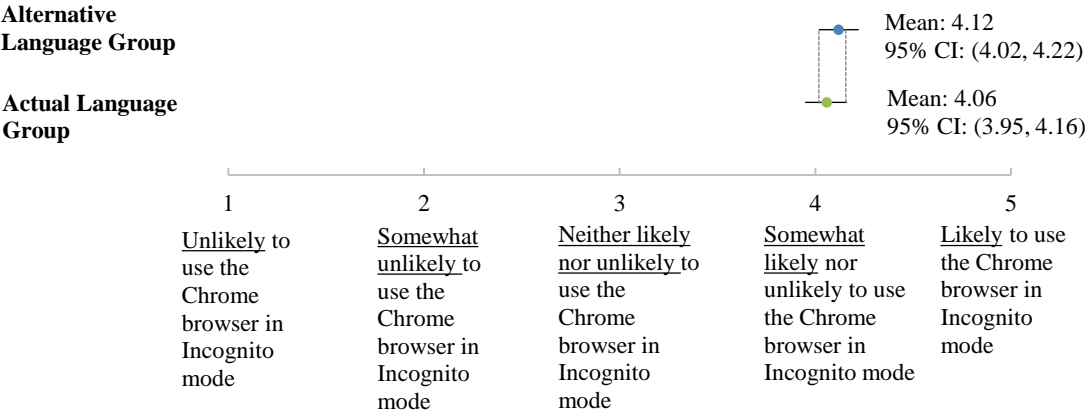
<sup>105</sup> My survey instrument is available in **Appendix F.3**.

<sup>106</sup> My results are robust to different sensitivity analyses. For example, I cut the sample by age group, gender, and region and the findings from my results still hold.

they were browsing privately”<sup>107</sup> does not have an impact on respondents’ likelihood of using Chrome.

**Figure 4. User Likelihood to Use Chrome in Incognito Mode**  
**Average Likelihood by Group**

“How likely or unlikely are you to use the Chrome browser in Incognito mode for your online research about the sensitive topic mentioned in the previous scenario?”



Notes:  
[1] The data points represent the mean values of the Actual Language and Alternative Language group responses to question 5.  
[2] Responses of “I don’t feel I have enough information to answer this question” were excluded in the calculation of means.

Source: **Exhibit 11.**

**Table 10. User Likelihood to Use Chrome in Incognito Mode**  
**Distribution by Group**

“How likely or unlikely are you to use the Chrome browser in Incognito mode for your online research about the sensitive topic mentioned in the previous scenario?”

1 = “Unlikely to use the Chrome browser in Incognito mode,”  
2 = “Somewhat unlikely to use the Chrome browser in Incognito mode,”  
3 = “Neither likely nor unlikely to use the Chrome browser in Incognito mode,”  
4 = “Somewhat likely to use the Chrome browser in Incognito mode,”  
5 = “Likely to use the Chrome browser in Incognito mode”)

	Actual Language Group n=503		Alternative Language Group n=502	
	#	%	#	%
Unlikely (1)	27	5%	25	5%
Somewhat unlikely (2)	26	5%	36	7%
Neither likely nor unlikely (3)	59	12%	33	7%
Somewhat likely (4)	155	31%	153	30%
Likely (5)	219	44%	240	48%
I don’t feel I have enough information to answer this question	17	3%	15	3%

Source: **Exhibit 12.**

84. For respondents in the Actual Language group, the average likelihood of using Chrome in Incognito mode to do online research on a sensitive topic is 4.06 (between *somewhat likely* and *likely*).<sup>108</sup> For respondents in the Alternative Language group, the average likelihood

<sup>107</sup> TAC, ¶ 53.

<sup>108</sup> **Figure 4** and **Exhibit 11.**

CONFIDENTIAL  
SUBJECT TO PROTECTIVE ORDER

- of using Chrome in Incognito mode to do online research on a sensitive topic is 4.12 (between *somewhat likely* and *likely*).<sup>109</sup> Using the t-test to assess significance, the difference between the means of the two groups is not statistically significant.<sup>110</sup>
85. Among respondents in the Actual Language group, 44% are *likely* (5 on the scale) to use Chrome in Incognito mode to do online research on a sensitive topic, and including those who answered *somewhat likely* (4 or 5 on the scale), the proportion of respondents is 74%.<sup>111</sup> Among respondents in the Alternative Language group, 48% are *likely* (5 on the scale) to use Chrome in Incognito mode to do online research on a sensitive topic, and including those who answered *somewhat likely* (4 or 5 on the scale), the proportion of respondents is 78%.<sup>112</sup> Using the two-tailed, two sample equality test of proportions to assess significance, which compares whether the proportions of two groups are the same, the proportion of respondents who answered *likely* (5 on the scale) in the Actual Language group is not statistically significantly different from the proportion of respondents who answered *likely* (5 on the scale) in the Alternative Language group.”<sup>113</sup> The proportion of respondents who answered *somewhat likely* or *likely* (4 or 5 on the scale) in the Actual Language group is also not statistically significantly different from the proportion of respondents who answered *somewhat likely* or *likely* (4 or 5 on the scale) in the Alternative Language group.”<sup>114, 115</sup>
86. The difference in likelihood to use Chrome in Incognito mode to do online research on a sensitive topic is not statistically significant between respondents in the Actual Language and Alternative Language groups, meaning the alternative language further clarifying that Incognito mode is designed to provide privacy from “other people who use this device,” and does not prevent web-service entities like Google from receiving their data, **has no**

---

<sup>109</sup> **Figure 4 and Exhibit 11.**

<sup>110</sup> **Exhibit 11.**

<sup>111</sup> **Table 10 and Exhibits 12 and 13.**

<sup>112</sup> **Table 10 and Exhibits 12 and 13.**

<sup>113</sup> **Exhibit 13.**

<sup>114</sup> **Exhibit 13.**

<sup>115</sup> The proportion of respondents who answered “I do not feel I have enough information to answer this question” in the Actual Language group is not statistically significantly different from the proportion of respondents who answered “I do not feel I have enough information to answer this question” in the Alternative Language group.

*CONFIDENTIAL*  
*SUBJECT TO PROTECTIVE ORDER*

impact on respondents' overall willingness to use Chrome in Incognito mode to do online research on a sensitive topic.

A handwritten signature in blue ink, consisting of a stylized 'A' followed by a long horizontal stroke.

---

On Amir

## Exhibit 1

### Consumer Perceptions and Expectations Survey Respondent Demographics

Demographic	Starts <sup>[1]</sup>		At QS8 <sup>[2]</sup>		Completes <sup>[3]</sup>	
	N	%	N	%	N	%
<i>Age</i>						
18-29	466	22%	315	21%	151	28%
30-39	397	19%	271	18%	123	23%
40-49	405	19%	307	20%	137	26%
50-59	353	17%	254	17%	76	14%
60+	460	22%	381	25%	44	8%
<b>Total</b>	2081	100%	1528	100%	531	100%
<i>Gender</i>						
Female	1064	51%	789	52%	251	47%
Male	1017	49%	738	48%	280	53%
Other	-	-	1	0%	-	-
<b>Total</b>	2081	100%	1528	100%	531	100%
<i>U.S. Region</i>						
Midwest	444	21%	343	22%	116	22%
Northeast	382	18%	271	18%	92	17%
South	788	38%	584	38%	211	40%
West	467	22%	330	22%	112	21%
<b>Total</b>	2081	100%	1528	100%	531	100%

#### Notes:

[1] Age, gender, and U.S. region distributions are calculated using the “NexusAge,” “NexusGender,” and “NexusRegion” variables, respectively. Responses with a missing value for any of the “NexusAge,” “NexusGender,” and “NexusRegion” variables are excluded.

[2] Age, gender, and U.S. region distributions are calculated using the “QS2,” “QS3,” and “Region\_US” variables, respectively, for all respondents who provided a response to “QS8. In the past six months, which of the following features, if any, have you used on your internet browser(s)?”

[3] Age, gender, and U.S. region distributions are calculated using the “QS2,” “QS3,” and “Region\_US” variables, respectively, for all respondents who completed the survey and are in the final analytical sample.

[4] All response options that do not result in termination from the survey are shown.

#### Source:

2203704.xlsx

## Exhibit 2

### Consumer Perceptions and Expectations Survey Response Statistics

Status	N	%
<i>Total Clicks</i> <sup>[1]</sup>	2,464	100%
<i>Completed Survey</i>	553	22%
Excluded by Survey Vendor <sup>[2]</sup>	22	1%
Final Analytical Sample	531	22%
<i>Screened Out of Survey</i>	1,738	71%
Overquota <sup>[3]</sup>	418	17%
RVID Dupes <sup>[4]</sup>	0	0%
At QS0 (Captcha)	2	0%
At QS2 (Age) / QS3 (Gender) <sup>[5]</sup>	184	7%
At QS4 (State) <sup>[6]</sup>	33	1%
At QS5 (Employment) <sup>[7]</sup>	56	2%
At QS6 (Attention) <sup>[8]</sup>	109	4%
At QS7 (Browser) <sup>[9]</sup>	11	0%
At QS8 (Browser Features) <sup>[10]</sup>	925	38%
<i>Dropped Out of Survey</i>	173	7%
During Screener	138	6%
After Screener	35	1%

#### Notes:

[1] The total number of people who clicked on the survey link is the sum of “Completed Survey,” “Screened Out of Survey,” and “Dropped Out of Survey.”

[2] Respondents were excluded from the final analytical sample by the survey vendor if they failed standard quality checks conducted by the survey vendor.

[3] Respondents were screened out of the survey if they exceeded the survey quotas.

[4] Duplicate responses were removed.

[5] Respondents were screened out at QS2 if they were under 18 years old, preferred not to answer, or if the age they indicated did not match the age on file with the survey vendor. Respondents were screened out at QS3 if they preferred not to answer or if they indicated “Male” or “Female” and their response did not match the gender on file with the survey vendor.

[6] Respondents were screened out at QS4 if they selected “Prefer not to answer” or “Don’t know / Unsure.”

[7] Respondents were screened out at QS5 if they or anyone else in their household has ever been employed by a law firm, legal services organization, or court.

[8] Respondents were screened out at QS6 if they selected a response option other than “South”.

[9] Respondents were screened out at QS7 if they indicated that they used the “Odeon” browser.

[10] Respondents were screened out at QS8 if they did not indicate that they have used “Private Browsing Mode” in the past six months.

#### Source:

2203704.xlsx



**Exhibit 3.1****Consumer Perceptions and Expectations Survey  
Response Counts**

*Q4. “While in [MODE NAME] mode, do the companies that own the websites you visited during the session receive or not receive the data from your [MODE NAME] session (such as IP address, URLs of the sites you visit, and cookies)?”*

	Chrome		Safari		Firefox		All Browsers	
	#	%	#	%	#	%	#	%
<b><i>Response Options</i></b>								
Companies that own the websites I visited during the session do not receive the data from my [MODE NAME] session (1)	40	15%	25	19%	24	19%	89	17%
Companies that own the websites I visited during the session probably do not receive the data from my [MODE NAME] session (2)	35	13%	24	18%	16	13%	75	14%
It is uncertain whether companies that own the websites I visited during the session receive the data from my [MODE NAME] session (3)	41	15%	22	16%	16	13%	79	15%
Companies that own the websites I visited during the session probably receive the data from my [MODE NAME] session (4)	66	24%	32	24%	24	19%	122	23%
Companies that own the websites I visited during the session do receive the data from my [MODE NAME] session (5)	67	25%	12	9%	37	29%	116	22%
I don't feel I have enough information to answer this question	21	8%	20	15%	9	7%	50	9%
<b>Total</b>	<b>270</b>	<b>100%</b>	<b>135</b>	<b>100%</b>	<b>126</b>	<b>100%</b>	<b>531</b>	<b>100%</b>

**Source:**

2203704.xlsx.

**Exhibit 3.2****Consumer Perceptions and Expectations Survey  
Response Counts**

*Q5. “While in [MODE NAME] mode, does your internet service provider receive or not receive the data from your [MODE NAME] session (such as IP address, URLs of the sites you visit, and cookies)?”*

	Chrome		Safari		Firefox		All Browsers	
	#	%	#	%	#	%	#	%
<b><i>Response Options</i></b>								
My internet service provider does not receive the data from my [MODE NAME] session (1)	42	16%	30	22%	18	14%	90	17%
My internet service provider probably does not receive the data from my [MODE NAME] session (2)	29	11%	25	19%	14	11%	68	13%
It is uncertain whether my internet service provider receives the data from my [MODE NAME] session or not (3)	44	16%	31	23%	14	11%	89	17%
My internet service provider probably receives the data from my [MODE NAME] session (4)	63	23%	28	21%	30	24%	121	23%
My internet service provider does receive the data from my [MODE NAME] session (5)	80	30%	13	10%	43	34%	136	26%
I don't feel I have enough information to answer this question	12	4%	8	6%	7	6%	27	5%
<b>Total</b>	<b>270</b>	<b>100%</b>	<b>135</b>	<b>100%</b>	<b>126</b>	<b>100%</b>	<b>531</b>	<b>100%</b>

**Source:**

2203704.xlsx.

**Exhibit 3.3****Consumer Perceptions and Expectations Survey  
Response Counts**

*Q6. “While in [MODE NAME] mode, do companies that provide analytics and advertising services to websites you visited during the session receive or not receive the data from your [MODE NAME] session (such as IP address, URLs of the sites you visit, and cookies)?”*

	Chrome		Safari		Firefox		All Browsers	
	#	%	#	%	#	%	#	%
<b><i>Response Options</i></b>								
Companies that provide analytics and advertising services to websites I visited during the session do not receive the data from my [MODE NAME] session (1)	55	20%	30	22%	29	23%	114	21%
Companies that provide analytics and advertising services to websites I visited during the session probably do not receive the data from my [MODE NAME] session (2)	40	15%	21	16%	12	10%	73	14%
It is uncertain whether companies that provide analytics and advertising services to websites I visited during the session receive the data from my [MODE NAME] session or not (3)	37	14%	30	22%	14	11%	81	15%
Companies that provide analytics and advertising services to websites I visited during the session probably receive the data from my [MODE NAME] session (4)	63	23%	26	19%	31	25%	120	23%
Companies that provide analytics and advertising services to websites I visited during the session do receive the data from my [MODE NAME] session (5)	57	21%	11	8%	31	25%	99	19%
I don't feel I have enough information to answer this question	18	7%	17	13%	9	7%	44	8%
<b>Total</b>	<b>270</b>	<b>100%</b>	<b>135</b>	<b>100%</b>	<b>126</b>	<b>100%</b>	<b>531</b>	<b>100%</b>

**Source:**

2203704.xlsx.

## Exhibit 4.1

### Consumer Perceptions and Expectations Survey Proportions of ‘Low’ Responses

*Q4-Q6. “While in [MODE NAME] mode, [do people or companies] receive or not receive the data from your [MODE NAME] session (such as IP address, URLs of the sites you visit, and cookies)?”*

	Chrome n = 270	All n = 531
<b><u>Companies that provide analytics and advertising services to websites you visited</u></b> <sup>[1][2]</sup>		
Proportion of respondents who answered 1 <sup>[1]</sup>	20%	21%
p-value at .3 threshold <sup>[5][6]</sup>	0.00***	0.00***
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	35%	35%
p-value at .5 threshold <sup>[5][7]</sup>	0.00***	0.00***
<b><u>Internet service provider</u></b> <sup>[1][3]</sup>		
Proportion of respondents who answered 1 <sup>[1]</sup>	16%	17%
p-value at .3 threshold <sup>[5][6]</sup>	0.00***	0.00***
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	26%	30%
p-value at .5 threshold <sup>[5][7]</sup>	0.00***	0.00***
<b><u>Companies that own the websites you visited</u></b> <sup>[1][4]</sup>		
Proportion of respondents who answered 1 <sup>[1]</sup>	15%	17%
p-value at .3 threshold <sup>[5][6]</sup>	0.00***	0.00***
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	28%	31%
p-value at .5 threshold <sup>[5][7]</sup>	0.00***	0.00***

**Notes:**

[1] Numerical values correspond to response options as follows: 1 = “[people or companies] do not receive the data from my [MODE NAME] session,” 2 = “[people or companies] probably do not receive the data from my [MODE NAME] session,” 3 = “It is uncertain whether [people or companies] receive the data from my [MODE NAME] session or not,” 4 = “[people or companies] probably receive the data from my [MODE NAME] session,” 5 = “[people or companies] do receive the data from my [MODE NAME] session.”

[2] Q6: Pipe in “do companies that provide analytics and advertising services to websites you visited during the session” for “[do people or companies].”

[3] Q5: Pipe in “does your internet service provider” for “[do people or companies].”

[4] Q4: Pipe in “do the companies that own the websites you visit” for “[do people or companies].”

[5] Symbols \*\*\*, \*\*, and \* represent statistical significance at the 1%, 5%, and 10% levels respectively.

[6] One-tailed, one sample equality test of proportions testing whether proportion of respondents who selected “[people or companies] do not receive the data from my [MODE NAME] session” is less than a hypothesized null threshold.

[7] One-tailed, one sample equality test of proportions testing whether proportion of respondents who selected “[people or companies] do not receive the data from my [MODE NAME] session” or “[people or companies] probably do not receive the data from my [MODE NAME] session” is less than a hypothesized null threshold.

[8] Responses of “I don’t feel I have enough information to answer this question” are included in all calculations.

**Source:**

2203704.xlsx.

## Exhibit 4.2

### Consumer Perceptions and Expectations Survey Proportions of ‘Low’ Responses vs Proportions of ‘High’ Responses

*Q4-Q6. “While in [MODE NAME] mode, [do people or companies] receive or not receive the data from your [MODE NAME] session (such as IP address, URLs of the sites you visit, and cookies)?”*

	Chrome n = 270	All n = 531
<b><u>Companies that provide analytics and advertising services to websites you visited</u></b> <sup>[1][2]</sup>		
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	35%	35%
Proportion of respondents who answered 4 or 5 <sup>[1]</sup>	44%	41%
Equivalence of proportions p-value <sup>[5][6]</sup>	0.01**	0.02**
<b><u>Internet service provider</u></b> <sup>[1][3]</sup>		
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	26%	30%
Proportion of respondents who answered 4 or 5 <sup>[1]</sup>	53%	48%
Equivalence of proportions p-value <sup>[5][6]</sup>	0.00***	0.00***
<b><u>Companies that own the websites you visited</u></b> <sup>[1][4]</sup>		
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	28%	31%
Proportion of respondents who answered 4 or 5 <sup>[1]</sup>	49%	45%
Equivalence of proportions p-value <sup>[5][6]</sup>	0.00***	0.00***

**Notes:**

[1] Numerical values correspond to response options as follows: 1 = “[people or companies] do not receive the data from my [MODE NAME] session,” 2 = “[people or companies] probably do not receive the data from my [MODE NAME] session,” 3 = “It is uncertain whether [people or companies] receive the data from my [MODE NAME] session or not,” 4 = “[people or companies] probably receive the data from my [MODE NAME] session,” 5 = “[people or companies] do receive the data from my [MODE NAME] session.”

[2] Q6: Pipe in “do companies that provide analytics and advertising services to websites you visited during the session” for “[do people or companies].”

[3] Q5: Pipe in “does your internet service provider” for “[do people or companies].”

[4] Q4: Pipe in “do the companies that own the websites you visit” for “[do people or companies].”

[5] Symbols \*\*\*, \*\*, and \* represent statistical significance at the 1%, 5%, and 10% levels respectively.

[6] One-tailed, two sample equality test of proportions testing whether proportion of respondents who selected “[people or companies] do not receive this information” or “[people or companies] probably do not receive this information” is less than proportion of respondents who selected “[people or companies] probably receive the data from my [MODE NAME] session” or “[people or companies] do receive the data from my [MODE NAME] session.”

[7] Responses of “I don't feel I have enough information to answer this question” are included in all calculations.

**Source:**

2203704.xlsx.

## Exhibit 5

### Interpretation Survey Respondent Demographics

Demographic	Starts <sup>[1]</sup>		At QS8 <sup>[2]</sup>		Completes <sup>[3]</sup>	
	N	%	N	%	N	%
<i>Age</i>						
18-29	1099	22%	680	19%	323	32%
30-39	954	19%	633	18%	254	25%
40-49	960	19%	691	19%	212	21%
50-59	779	16%	577	16%	125	12%
60+	1229	24%	972	27%	99	10%
<b>Total</b>	5021	100%	3553	100%	1013	100%
<i>Gender</i>						
Female	2771	55%	2027	57%	485	48%
Male	2250	45%	1516	43%	521	51%
Other	-	-	10	0%	7	1%
<b>Total</b>	5021	100%	3553	100%	1013	100%
<i>U.S. Region</i>						
Midwest	1097	22%	771	22%	213	21%
Northeast	884	18%	610	17%	148	15%
South	1983	39%	1434	40%	396	39%
West	1057	21%	738	21%	256	25%
<b>Total</b>	5021	100%	3553	100%	1013	100%

#### Notes:

[1] Age, gender, and U.S. region distributions are calculated using the “NexusAge,” “NexusGender,” and “NexusRegion” variables, respectively. Responses with a missing value for any of the “NexusAge,” “NexusGender,” and “NexusRegion” variables are excluded.

[2] Age, gender, and U.S. region distributions are calculated using the “QS2,” “QS3,” and “Region\_US” variables, respectively, for all respondents who provided a response to “QS8. In the past six months, which of the following features, if any, have you used on your internet browser(s)?”

[3] Age, gender, and U.S. region distributions are calculated using the “QS2,” “QS3,” and “Region\_US” variables, respectively, for all respondents who completed the survey and are in the final analytical sample.

[4] All response options that do not result in termination from the survey are shown.

#### Source:

2203487.xlsx

## Exhibit 6

### Interpretation Survey Response Statistics

Status	N	%
<i>Total Clicks</i> <sup>[1]</sup>	5,198	100%
<i>Completed Survey</i>	1,109	21%
Excluded by Survey Vendor <sup>[2]</sup>	96	2%
Final Analytical Sample	1,013	19%
<i>Screened Out of Survey</i>	3,592	69%
Overquota <sup>[3]</sup>	120	2%
RVID Dupes <sup>[4]</sup>	0	0%
At QS0 (Captcha)	113	2%
At QS2 (Age) / QS3 (Gender) <sup>[5]</sup>	519	10%
At QS4 (State) <sup>[6]</sup>	86	2%
At QS5 (Employment) <sup>[7]</sup>	150	3%
At QS6 (Attention) <sup>[8]</sup>	233	4%
At QS7 (Browser) <sup>[9]</sup>	47	1%
At QS8 (Browser Features) <sup>[10]</sup>	2,324	45%
<i>Dropped Out of Survey</i>	497	10%
During Screener	379	7%
After Screener	118	2%

#### Notes:

[1] The total number of people who clicked on the survey link is the sum of “Completed Survey,” “Screened Out of Survey,” and “Dropped Out of Survey.”

[2] Respondents were excluded from the final analytical sample by the survey vendor if they failed standard quality checks conducted by the survey vendor.

[3] Respondents were screened out of the survey if they exceeded the survey quotas.

[4] Duplicate responses were removed.

[5] Respondents were screened out at QS2 if they were under 18 years old, preferred not to answer, or if the age they indicated did not match the age on file with the survey vendor. Respondents were screened out at QS3 if they preferred not to answer or if they indicated “Male” or “Female” and their response did not match the gender on file with the survey vendor.

[6] Respondents were screened out at QS4 if they selected “Prefer not to answer” or “Don’t know / Unsure.”

[7] Respondents were screened out at QS5 if they or anyone else in their household has ever been employed by a law firm, legal services organization, or court.

[8] Respondents were screened out at QS6 if they selected a response option other than “South”.

[9] Respondents were screened out at QS7 if they indicated that they used the “Odeon” browser.

[10] Respondents were screened out at QS8 if they did not indicate that they have used “Private Browsing Mode” in the past six months.

#### Source:

2203487.xlsx



**Exhibit 7.1****Interpretation Survey  
Response Counts**

*Q10. “Based on the screens that you reviewed, please select one of the following regarding URLs of the sites you visit during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product):”*

	Splash Screen Only		Splash Screen with Policies (Highlighted)		Splash Screen with New Account Creation Agreement		Splash Screen with Consent Bump Agreement and FAQ Page	
	#	%	#	%	#	%	#	%
<b><i>Response Options</i></b>								
Google does not receive this information (1)	33	13%	47	19%	35	14%	43	17%
Google probably does not receive this information (2)	34	13%	22	9%	29	12%	31	12%
It is uncertain whether Google receives this information or not (3)	35	14%	23	9%	31	12%	16	6%
Google probably receives this information (4)	69	27%	52	20%	58	23%	77	30%
Google does receive this information (5)	68	27%	87	34%	74	29%	62	25%
I don't feel I have enough information to answer this question	15	6%	23	9%	25	10%	24	9%
<b>Total by Group</b>	<b>254</b>	<b>100%</b>	<b>254</b>	<b>100%</b>	<b>252</b>	<b>100%</b>	<b>253</b>	<b>100%</b>

**Source:**

2203487.xlsx.

**Exhibit 7.2****Interpretation Survey  
Response Counts**

*Q11. “Based on the screens that you reviewed, please select one of the following regarding IP address during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product):”*

	Splash Screen Only		Splash Screen with Policies (Highlighted)		Splash Screen with New Account Creation Agreement		Splash Screen with Consent Bump Agreement and FAQ Page	
	#	%	#	%	#	%	#	%
<b><i>Response Options</i></b>								
Google does not receive this information (1)	14	6%	30	12%	20	8%	25	10%
Google probably does not receive this information (2)	21	8%	19	7%	22	9%	25	10%
It is uncertain whether Google receives this information or not (3)	28	11%	19	7%	30	12%	26	10%
Google probably receives this information (4)	70	28%	68	27%	62	25%	75	30%
Google does receive this information (5)	95	37%	92	36%	99	39%	81	32%
I don't feel I have enough information to answer this question	26	10%	26	10%	19	8%	21	8%
<b>Total</b>	<b>254</b>	<b>100%</b>	<b>254</b>	<b>100%</b>	<b>252</b>	<b>100%</b>	<b>253</b>	<b>100%</b>

**Source:**

2203487.xlsx.

**Exhibit 7.3****Interpretation Survey****Response Counts**

*Q12. “Based on the screens that you reviewed, please select one of the following regarding cookies placed on your browser during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product):”*

	Splash Screen Only		Splash Screen with Policies (Highlighted)		Splash Screen with New Account Creation Agreement		Splash Screen with Consent Bump Agreement and FAQ Page	
	#	%	#	%	#	%	#	%
<b><i>Response Options</i></b>								
Google does not receive this information (1)	59	23%	53	21%	43	17%	64	25%
Google probably does not receive this information (2)	37	15%	28	11%	31	12%	32	13%
It is uncertain whether Google receives this information or not (3)	26	10%	10	4%	29	12%	15	6%
Google probably receives this information (4)	60	24%	58	23%	55	22%	58	23%
Google does receive this information (5)	57	22%	82	32%	68	27%	67	26%
I don't feel I have enough information to answer this question	15	6%	23	9%	26	10%	17	7%
<b>Total</b>	<b>254</b>	<b>100%</b>	<b>254</b>	<b>100%</b>	<b>252</b>	<b>100%</b>	<b>253</b>	<b>100%</b>

**Source:**

2203487.xlsx.

## Exhibit 8.1

### Interpretation Survey Proportions of “Low” Responses by Group

*Q10-12 “Based on the screens that you saw, please select one of the following regarding [data types] during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product):”*

	Splash Screen Only	Splash Screen with Policies (Highlighted)	Splash Screen with New Account Creation Agreement	Splash Screen with Consent Bump Agreement and FAQ Page
	n = 254	n = 254	n = 252	n = 253
<b><u>URLs of the sites you visit</u></b>				
Proportion of respondents who answered 1 <sup>[1]</sup>	13%	19%	14%	17%
p-value at .3 threshold <sup>[2][3]</sup>	0.00***	0.00***	0.00***	0.00***
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	26%	27%	25%	29%
p-value at .5 threshold <sup>[2][4]</sup>	0.00***	0.00***	0.00***	0.00***
<b><u>IP address</u></b>				
Proportion of respondents who answered 1 <sup>[1]</sup>	6%	12%	8%	10%
p-value at .3 threshold <sup>[2][3]</sup>	0.00***	0.00***	0.00***	0.00***
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	14%	19%	17%	20%
p-value at .5 threshold <sup>[2][4]</sup>	0.00***	0.00***	0.00***	0.00***
<b><u>Cookies placed on your browser</u></b> <sup>[1]</sup>				
Proportion of respondents who answered 1 <sup>[1]</sup>	23%	21%	17%	25%
p-value at .3 threshold <sup>[2][3]</sup>	0.01***	0.00***	0.00***	0.05*
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	38%	32%	29%	38%
p-value at .5 threshold <sup>[2][4]</sup>	0.00***	0.00***	0.00***	0.00***

**Notes:**

[1] Numerical values correspond to response options as follows: 1 = “Google does not receive this information,” 2 = “Google probably does not receive this information,” 3 = “It is uncertain whether Google receives this information or not,” 4 = “Google probably receives this information,” 5 = “Google does receive this information.”

[2] Symbols \*\*\*, \*\*, and \* represent statistical significance at the 1%, 5%, and 10% levels respectively.

[3] One-tailed, one sample equality test of proportions testing whether proportion of respondents who selected “Google does not receive this information” is less than a hypothesized null threshold.

[4] One-tailed, one sample equality test of proportions testing whether proportion of respondents who selected “Google does not receive this information” or “Google probably does not receive this information” is less than a hypothesized null threshold.

[5] Responses of “I don't feel I have enough information to answer this question” are included in the denominator for the calculations of proportions.

**Source:**

2203487.xlsx.

## Exhibit 8.2

### Interpretation Survey

#### Proportions of “Low” Responses vs Proportions of “High” Responses

*Q10-12 “Based on the screens that you saw, please select one of the following regarding [data types] during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product):”*

	Splash Screen Only	Splash Screen with Policies (Highlighted)	Splash Screen with New Account Creation Agreement	Splash Screen with Consent Bump Agreement and FAQ Page
	n = 254	n = 254	n = 252	n = 253
<b><u>URLs of the sites you visit</u></b>				
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	26%	27%	25%	29%
Proportion of respondents who answered 4 or 5 <sup>[1]</sup>	54%	55%	52%	55%
Equivalence of proportions p- value <sup>[2][3]</sup>	0.00***	0.00***	0.00***	0.00***
<b><u>IP address</u></b>				
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	14%	19%	17%	20%
Proportion of respondents who answered 4 or 5 <sup>[1]</sup>	65%	63%	64%	62%
Equivalence of proportions p- value <sup>[2][3]</sup>	0.00***	0.00***	0.00***	0.00***
<b><u>Cookies placed on your browser</u><sup>[1]</sup></b>				
Proportion of respondents who answered 1 or 2 <sup>[1]</sup>	38%	32%	29%	38%
Proportion of respondents who answered 4 or 5 <sup>[1]</sup>	46%	55%	49%	49%
Equivalence of proportions p- value <sup>[2][3]</sup>	0.03**	0.00***	0.00***	0.00***

**Notes:**

[1] Numerical values correspond to response options as follows: 1 = “Google does not receive this information,” 2 = “Google probably does not receive this information,” 3 = “It is uncertain whether Google receives this information or not,” 4 = “Google probably receives this information,” 5 = “Google does receive this information.”

[2] Symbols \*\*\*, \*\*, and \* represent statistical significance at the 1%, 5%, and 10% levels respectively.

[3] One-tailed, two sample equality test of proportions testing whether proportion of respondents who selected “Google does not receive this information” or “Google probably does not receive this information” is less than the proportion of respondents who selected “Google does receive this information” or “Google probably receives this information.”

[4] Responses of “I don't feel I have enough information to answer this question” are included in the denominator for the calculations of proportions.

**Source:**

2203487.xlsx.

## Exhibit 9

### Likelihood of Use Survey Respondent Demographics

Demographic	Starts <sup>[1]</sup>		At QS8 <sup>[2]</sup>		Completes <sup>[3]</sup>	
	N	%	N	%	N	%
<i>Age</i>						
18-29	867	22%	603	20%	312	31%
30-39	687	17%	456	15%	205	20%
40-49	749	19%	571	19%	212	21%
50-59	693	17%	521	18%	149	15%
60+	998	25%	818	28%	127	13%
<b>Total</b>	3994	100%	2969	100%	1005	100%
<i>Gender</i>						
Female	2072	52%	1608	54%	505	50%
Male	1922	48%	1359	46%	500	50%
Other	-	-	2	0%	-	-
<b>Total</b>	3994	100%	2969	100%	1005	100%
<i>U.S. Region</i>						
Midwest	866	22%	667	22%	218	22%
Northeast	702	18%	505	17%	173	17%
South	1520	38%	1162	39%	375	37%
West	906	23%	635	21%	239	24%
<b>Total</b>	3994	100%	2969	100%	1005	100%

#### Notes:

[1] Age, gender, and U.S. region distributions are calculated using the “NexusAge,” “NexusGender,” and “NexusRegion” variables, respectively. Responses with a missing value for any of the “NexusAge,” “NexusGender,” and “NexusRegion” variables are excluded.

[2] Age, gender, and U.S. region distributions are calculated using the “QS2,” “QS3,” and “Region\_US” variables, respectively, for all respondents who provided a response to “QS8. In the past six months, which of the following features, if any, have you used on your internet browser(s)?”

[3] Age, gender, and U.S. region distributions are calculated using the “QS2,” “QS3,” and “Region\_US” variables, respectively, for all respondents who completed the survey and are in the final analytical sample.

[4] All response options that do not result in termination from the survey are shown.

#### Source:

2203523.xlsx

## Exhibit 10

### Likelihood of Use Survey Response Statistics

Status	N	%
<i>Total Clicks</i> <sup>[1]</sup>	4,015	100%
<i>Completed Survey</i>	1,104	27%
Excluded by Survey Vendor <sup>[2]</sup>	99	2%
Final Analytical Sample	1,005	25%
<i>Screened Out of Survey</i>	2,665	66%
Overquota <sup>[3]</sup>	0	0%
RVID Dupes <sup>[4]</sup>	2	0%
At QS0 (Captcha)	17	0%
At QS2 (Age) / QS3 (Gender) <sup>[5]</sup>	423	11%
At QS4 (State) <sup>[6]</sup>	44	1%
At QS5 (Employment) <sup>[7]</sup>	97	2%
At QS6 (Attention) <sup>[8]</sup>	210	5%
At QS7 (Browser) <sup>[9]</sup>	49	1%
At QS8 (Browser Features) <sup>[10]</sup>	1,823	45%
<i>Dropped Out of Survey</i>	246	6%
During Screener	204	5%
After Screener	42	1%

#### Notes:

[1] The total number of people who clicked on the survey link is the sum of “Completed Survey,” “Screened Out of Survey,” and “Dropped Out of Survey.”

[2] Respondents were excluded from the final analytical sample by the survey vendor if they failed standard quality checks conducted by the survey vendor.

[3] Respondents were screened out of the survey if they exceeded the survey quotas.

[4] Duplicate responses were removed.

[5] Respondents were screened out at QS2 if they were under 18 years old, preferred not to answer, or if the age they indicated did not match the age on file with the survey vendor. Respondents were screened out at QS3 if they preferred not to answer or if they indicated “Male” or “Female” and their response did not match the gender on file with the survey vendor.

[6] Respondents were screened out at QS4 if they selected “Prefer not to answer” or “Don’t know / Unsure.”

[7] Respondents were screened out at QS5 if they or anyone else in their household has ever been employed by a law firm, legal services organization, or court.

[8] Respondents were screened out at QS6 if they selected a response option other than “South”.

[9] Respondents were screened out at QS7 if they indicated that they used the “Odeon” browser.

[10] Respondents were screened out at QS8 if they did not indicate that they have used “Private Browsing Mode” in the past six months.

#### Source:

2203523.xlsx



**Exhibit 11****Likelihood of Use Survey  
Mean and 95 % Confidence Interval**

*Q5. “How likely or unlikely are you to use the Chrome browser in Incognito mode for your online research about the sensitive topic mentioned in the previous scenario?”*

Alternative Language Group				Actual Language Group				Mean Difference t-test p-value <sup>[2][3]</sup>
95% Confidence Interval				95% Confidence Interval				
N	Mean	Lower Bound	Upper Bound	N	Mean	Lower Bound	Upper Bound	
502	4.12	4.02	4.22	503	4.06	3.95	4.16	0.35

**Notes:**

[1] Numerical values correspond to response options as follows: 1 = “Unlikely to use the Chrome browser in Incognito mode,” 2 = “Somewhat unlikely to use the Chrome browser in Incognito mode,” 3 = “Neither likely nor unlikely to use the Chrome browser in Incognito mode,” 4 = “Somewhat likely to use the Chrome browser in Incognito mode,” 5 = “Likely to use the Chrome browser in Incognito mode.”

[2] Symbols \*\*\*, \*\*, and \* represent statistical significance at the 1%, 5%, and 10% levels respectively.

[3] Two-tailed Student's t-test.

[4] Responses of “I do not feel I have enough information to answer this question” are excluded from all calculations.

**Source:**

2203523.xlsx.

**Exhibit 12****Likelihood of Use Survey****Response Counts**

*Q5. "How likely or unlikely are you to use the Chrome browser in Incognito mode for your online research about the sensitive topic mentioned in the previous scenario?"*

<b>Response Options</b>	<b>Alternative Language</b>		<b>Actual Language</b>	
	<b>#</b>	<b>%</b>	<b>#</b>	<b>%</b>
Unlikely to use the Chrome browser in Incognito mode (1)	25	5%	27	5%
Somewhat unlikely to use the Chrome browser in Incognito mode (2)	36	7%	26	5%
Neither likely nor unlikely to use the Chrome browser in Incognito mode (3)	33	7%	59	12%
Somewhat likely to use the Chrome browser in Incognito mode (4)	153	30%	155	31%
Likely to use the Chrome browser in Incognito mode (5)	240	48%	219	44%
I don't feel I have enough information to answer this question	15	3%	17	3%
<b>Total</b>	<b>502</b>	<b>100%</b>	<b>503</b>	<b>100%</b>

**Source:**

2203523.xlsx.

**Exhibit 13****Likelihood of Use Survey**

*Q5. “How likely or unlikely are you to use the Chrome browser in Incognito mode for your online research about the sensitive topic mentioned in the previous scenario?”*

	<b>Alternative Language Group</b>	<b>Actual Language Group</b>	<b>Alternative vs. Actual Language proportion test <i>p</i> -value<sup>[1][2]</sup></b>
	<b>n = 502</b>	<b>n = 503</b>	
Proportion who responded 5 <sup>[3]</sup>	48%	44%	0.17
Proportion who responded 4 or 5 <sup>[4]</sup>	78%	74%	0.14

**Notes:**

[1] Numerical values correspond to response options as follows: 1 = “Unlikely to use the Chrome browser in Incognito mode,” 2 = “Somewhat unlikely to use the Chrome browser in Incognito mode,” 3 = “Neither likely nor unlikely to use the Chrome browser in Incognito mode,” 4 = “Somewhat likely to use the Chrome browser in Incognito mode,” 5 = “Likely to use the Chrome browser in Incognito mode.”

[2] Symbols \*\*\*, \*\*, and \* represent statistical significance at the 1%, 5%, and 10% levels respectively.

[3] Two-tailed, two-sample equality of proportion test comparing proportion of respondents who selected “Likely to use the Chrome browser in Incognito mode” between the alternative and actual language groups.

[4] Two-tailed, two-sample equality of proportion test comparing proportion of respondents who selected “Likely to use the Chrome browser in Incognito mode” or “Somewhat likely to use the Chrome browser in Incognito mode” between the alternative and actual language groups.

[5] Responses of “I do not feel I have enough information to answer this question” are included in all calculations.

**Source:**

2203523.xlsx.

# **APPENDIX A**

## **CURRICULUM VITAE**

***On Amir***

Rady School of Management  
University of California, San Diego  
Wells Fargo Hall  
9500 Gilman Drive, MC 0553  
La Jolla, CA 92093-0553  
(858) 534-2023  
[oamir@ucsd.edu](mailto:oamir@ucsd.edu)

---

***Education***

Ph.D., Management Science, Marketing, Massachusetts Institute of Technology  
B.S., Computer Science, Israeli Open University, Tel Aviv

***Academic Employment***

2020 – present	Wolfe Family Presidential Endowed Chair in Life Sciences, Innovation, and Entrepreneurship, Professor of Marketing Rady School of Management, University of California, San Diego,
2018 - 2021	Associate Dean of Programs Rady School of Management, University of California, San Diego
2018 – 2020	Professor of Marketing Rady School of Management, University of California, San Diego
2010 – 2017	Associate Professor of Marketing Rady School of Management, University of California, San Diego
2012 – 2013	Visiting Associate Professor of Marketing Kellogg School of Management, Northwestern University
2011 – 2012	Visiting Professor of Marketing Arison School of Management, IDC
2005 – 2010	Assistant Professor of Marketing Rady School of Management, University of California, San Diego
2003 – 2005	Assistant Professor of Marketing School of Management, Yale University

***Other Employment***

2018 - present	Chief Behavioral Science Officer, Fiverr, Inc.
1991 – 1999	Israeli Air Force

## ***Publications***

- Kristen Duke & On Amir (forthcoming). The Importance of Selling Formats: When Integrating Purchase and Quantity Decisions Increases Sales, *Marketing Science*.
- Evan Weingarten, Kristen Duke, Wendy liu, Rrebecca Hamilton, On Amir, Gil Apple, Moran Cerf, Joe Goodman, Andrea Morales, Ed O'Brian, Jordi Quidbach, & Monic Sun (forthcoming). What Makes People Happy? Decoupling the Experiential-Material Continuum, *Journal of Consumer Psychology*.
- Alicea Lieberman, Juliana Schroeder, & On Amir (forthcoming). A Voice Inside My Head: The Psychological and Behavioral Consequences of Auditory Technologies, Organization Behavior and Human Decision Processes.
- Alicea Lieberman, Andera Morales, & On Amir (forthcoming). Tangential Immersion: Increasing Consumer Persistence, *Journal or Consumer Research*.
- Coby Morvinski, Silvia Saccardo, & On Amir (forthcoming). Mis-Nudging Morality, *Management Science*
- Elanor Williams, Allie Lieberman, & On Amir (2021). Perspective Neglect: Inadequate Perspective Taking Limits Coordination, Judgment and Decision Making, 16 (4), 898-931.
- Weingarten, Evan, Michael W. Meyer, Amit Ashkenazi, & On Amir (2020). Experts Outperform Technology in Creative Markets, She Ji: The Journal of Design, Economics, and Innovation.
- Alicea Lieberman , Kristen Duke, & On Amir (2019). How Incentive Framing Can Harness the Power of Norms, Organizational Behavior & Human Decision Processes.
- Kristen E. Duke & On Amir (2019). Guilt Dynamics: Consequences of Temporally Separating Decisions and Actions, Journal of Consumer Research.
- On Amir, Nina Mazar, & Dan Ariely (2019). Replicating the Effect of Moral Standards Accessibility on Dishonesty, Author's Response to the Replication Process, Advances in Methods and Practices in Psychological Science.
- Raphael Thomadsen, Robert P. Roederkerk, On Amir, Neeraj Arora, Bryan Bollinger, Karsten Hansen, Leslie John, Wendy Liu, Aner Sela, Vishal Singh, K. Sudhir, & Wendy Wood (2018). How Context Affects Choice, Customer Needs and Solutions, 1-2, 3-14.
- Kristen Duke, Kelly Goldsmith, & On Amir (2018). Is the Preference for Certainty Always so Certain?, Journal of the Association of Consumer Research, 3(1), 63-80.
- Coby Morvinski & On Amir (2018). Liking Goes with Liking: An Intuitive Congruence between Preference and Prominence, Journal of Experimental Psychology: Learning, Memory, and Cognition.
- Daniella Kupor, Wendy Liu, & On Amir (2017). The Effect of an Interruption on Risk Decisions, Journal of Consumer Research, 44 (6), 1205–1219.

- Andrea Morales, On Amir, & Leonard Lee (2017). A Tutorial in Consumer Research: Keeping it Real in Experimental Research – Understanding When, Where, and How to Enhance Realism and Measure Consumer Behavior, Journal of Consumer Research, 44 (2), 465–476.
- Kerem Shuval, Tammy Leonard, Jeffrey Drope, David L. Katz, Alpa V. Patel, Melissa Maitin-Shepard, On Amir, & Amir Grinstein, (2017). Physical Activity Counseling in Primary Care: Insights from Public Health & Behavioral Economics, CA: A Cancer Journal for Clinicians, 67(3), 233-244.
- Coby Morvinski, On Amir, & Eitan Muller (2017). “Ten Million Readers Can’t Be Wrong!,” or Can They? On the Role of Information About Adoption Stock in New Product Trial, Marketing Science, 36(2), 290-300.
- On Amir and Orly Lobel (2014). How Non-Competes Stifle Performance, Harvard Business Review, 92 (1/2), p.26.
- On Amir and Orly Lobel (2013). Driving Performance: A Growth Theory of Non-Compete Law, Stanford Technology Law Review, 16 (3), spring.
- On Amir and Orly Lobel (2012). Liberalism and Lifestyle: Informing Regulatory Governance with Behavioral Research, European Journal of Risk Regulation, 1, 17-25.
- Kelly Goldsmith and On Amir (2010). Can Uncertainty Improve Promotions, Journal of Marketing Research, December, 1070-1077.
- Leonard Lee, On Amir, and Dan Ariely (2009). In Search of Homo Economicus: Cognitive Noise and the Role of Emotion in Preference Consistency, Journal of Consumer Research, 36, 173-187.
- Anastasiya Pocheptsova, On Amir, Ravi Dhar, and Roy Baumeister (2009). Deciding without Resources: Psychological Depletion and Choice in Context, Journal of Marketing Research, June, 46 (3), 344-355.
- On Amir and Dan Ariely (2008). Resting on Laurels: The Effects of Discrete Progress Markers as SubGoals on Task Performance and Preferences, Journal of Experimental Psychology: Learning, Memory, & Cognition, 34 (5), 1158-1171.
- On Amir and Orly Lobel (2008). Stumble, Predict, Nudge: How Behavioral Economics Informs Law and Policy, Columbia Law Review, December, 2098-2138.
- Nina Mazar, On Amir, and Dan Ariely (2008). The Dishonesty of Honest People: A Theory of Self-Concept Maintenance, Journal of Marketing Research, November, 45 (6), 633-644, (lead article).
- \*Media coverage: NY Times Science section (Nov. 20th, 2007)
- \*HBR Breakthrough Ideas for 2008.
- \*Winner of the 2012 William F. O’Dell award.
- Nina Mazar, On Amir, and Dan Ariely (2008). More Ways to Cheat – Expanding the Scope of Dishonesty, Journal of Marketing Research, November, 45 (6), 651-653.
- On Amir and Jonathan Levav (2008). Preference construction versus choice construction: The instability of preferences learned in context. Journal of Marketing Research, April, 145-158.



- On Amir, Ziv Carmon, and Dan Ariely (2008). The Dissociation between Monetary Assessments and Predicted Utility, Marketing Science, 27 (6), 1055-1064.
- On Amir and Dan Ariely (2007). Decisions by Rules: The Case of Unwillingness to Pay for Beneficial Delays. Journal of Marketing Research, February, 142-152.
- On Amir, Dan Ariely, Alan Cooke, David Dunning, Nicholas Epley, Botond Koszegi, Donald Lichtenstein, Nina Mazar, Sendhil Mullainathan, Drazen Prelec, Eldar Shafir, Jose Silva (2005). Behavioral Economics, Psychology, and Public Policy. Marketing Letters (Special Issue for the Sixth Choice Symposium), 16:3/4, 443-454.

### ***Other Publications***

- Alicia Lieberman, Andrea C. Morales, and On Amir (2019). Beyond the Lab: Using Data from the Field to Increase Research Validity, in Handbook of Research Methods in Consumer Psychology, Frank R. Kardes, Paul M. Herr, and Nobert Schwarz, Editors, Routledge.
- “Is the Mind like a Muscle?” Scientific American, Mind, online edition.
- “Making Consumption Decisions by Following Personal Rules”, In Inside Consumption: Frontiers of Research on Consumer Motives, Goals, and Desires. Ratti Ratneshwar & David Mick (eds.), Routledge Press 2005. (with Dan Ariely & Orly Lobel)
- On Amir & Ariely Dan (2001) e-Rationality: Rationality in Electronic Environments. In S.M. Broniarczyk, & K. Nakamoto, Advances in Consumer Research, 24. Provo, UT.
- On Amir (2004) Alternative Decision Processes in Consumption: Personal Rules, Rationales, and Identity Maintenance, Advances in Consumer Research, XXXI, 26.
- 

### ***Selected Research in Progress***

- Goal Proximity, Social Information, and Giving: When Norms Backfire (with Coby Morvinski and Matt Lupoli) – revision invited Journal of Marketing
- The Entrenchment Effect (with Allie Lieberman and Ziv Carmon) – Under review at Journal of Marketing Research
- How Different Encoding Processes Influence Confidence (with Giulia Maimone and Uma Karmarkar) – Under review at Journal of Experimental Psychology: Learning, Memory, and Cognition
- The most Influential Age Hypothesis: Does the Self Cause Predictable Preferences (with Nina Mazar) – revision invited Management Science.
- Reference Escalation in Sequential Choice (with Coby Morvinski) – under review Marketing Science
- My Experience or My Expectations: The Effect of Expectations as Reference Points on Evaluations of Experiential Purchases (with Amar Cheema, Davide Proserpio, and Stephanie Tully) – under review Journal of Consumer Research.

Risk Aversion as Self Control (with Orly Lobel and Kelly Goldsmith)

Driving Pro-Environmental Choice (with Elizabeth A. Keenan and Ayelet Gneezy)

Risk Management for the Future: Age, Risk, and Choice Architecture (with Orly Lobel)

---

### ***Honors and Awards***

MSI Research Award: “Do Experts Outperform Artificial Intelligence? The Case of Logo Design,” # 4000657, 2019

MSI Research Award: “Quantity Integration,” #4000477, 2018

MSI Research Award: “New Product Adoption,” #4-1842, 2014

Robert Woods Johnson Foundation research grant for Healthy Choices.

MSI Junior Scholars 2009

“Most Valuable Professor Award,” voted by the Flex MBA class of 2007

“Most Valuable Professor Award,” voted by the Fulltime MBA class of 2007

MSI Research Award: “Motivating Discounts: Price Motivated Consumer Reasoning”, #4-1273, 2004

AMA - Sheth Doctoral Consortium Fellow, 2002

MSI Research Award: “Information Aversion: Indecision, Procrastination, and Consumer Choice Online”, #4-1141, 2001

CS Holding Fellowship, 2001

Walter A Rosenblith Fellowship, 2000

---

### ***Conference presentations and Invited Talks***

University of California, Berkeley, Haas (2015)

University of Toronto, Rotman (2015)

University of Southern California, Marshal (2014)

University of Southern California, Psychology (2013)

University of Pennsylvania, Wharton (2007, 2013)

University of Chicago, Booth (2013)

Northwestern University, Kellogg (2012)

Interdisciplinary Center, Arison (2011)

Tel Aviv University, Recanati, Coller (2008, 2009, 2018)

Stanford University, GSB (2009)

Columbia University, GSB (2009)

University of California, San Diego, Psychology (2005, 2006, 2007, 2008)

University of California, San Diego, Economics (2008)

Erasmus University (2008)

University of Melbourne (2007)

Hebrew University (2007)

Washington University, St. Louis (2007)

University of San Diego, School of Law (2006)

University of California, Los Angeles, Anderson (2004)  
Yale University, Psychology (2004)  
INSEAD (2004, 2015)  
Johns Hopkins University (2017)  
NUS (2018)  
Ben Gurion University (2018)  
HKU (2019)  
CUHK (2019)

Association for Consumer Research, 2001, 2003, 2004, 2006, 2007, 2013, 2015, 2016  
Society of Consumer Psychology, 2004, 2005, 2008, 2012, 2014, 2015, 2016, 2017  
Society for Judgement and Decision Making, 2003, 2005, 2006, 2011, 2015, 2016  
Behavioral Decision Making Research in Management, 2002, 2006, 2008, 2014, 2016, 2018  
FUR, IESE, 2008  
Marketing in Israel, 2002, 2003, 2005  
Northeastern Marketing Consortium 2003  
Collier Conference of Behavioral Economics 2017, 2019  
DMEP 2019

---

### ***In the Media***

Decision Making Traps and Tips for Negotiators, CIIAN, December, 2021  
2021's Best Things to Buy on Black Friday, WalletHub, November 19, 2021  
'That's not true.' San Diego doctors tackle COVID misinformation sown during county meeting.  
San Diego Union Tribune, October 6, 2021  
You could be one of three San Diegans who just won \$50,000 in the state's vaccine lottery. San  
Diego Union Tribune, June 4, 2021.  
California's vaccine incentives program – KPBS, May 2021.  
San Diego health systems ask for fewer vaccine doses, turn down extra amid supply glut. San  
Diego Union Tribune, May 10, 2021.  
2021's Best Pleaces for Valentine's Day. WalletHub, February 2, 2021.  
We're getting closer to having a Covid-19 vaccine. Hold onto that mask, though. San Diego  
Union Tribune, October 25, 2020  
Psychology of Pricing: How to Price you Products Effectively, The Do List, May 23, 2019  
The Celebrity of Legalized Cannabis, Pacific San Diego, May 20, 2019  
Marines may ditch 'The Few, the Proud' slogan, San Diego Union Tribune, October 11, 2016  
The free-shipping wars have begun, San Diego Union Tribune, October 2013  
The Young and The Promising, TheMarker magazine, 2011  
Consumer Emotional Reactions to Changing Gas Prices, Ch. 10 News, August 2008  
Jogging Down the Comeback Trail, San Diego Union Tribune, August 2007  
Big Business and the Consumer, Jeremy Seville Comedy Hour, WealthTV 2007  
Social Marketing, San Diego Union Tribune, May 2007  
Trends in E-commerce, San Diego Business Journal, July 2006  
Dating websites, San Diego Union Tribune, April 2006  
Database marketing, Campus Technology, November 2005

Christmas shopping, Hartford Courant, December 2004

---

***Service***

*PhD Committee*

Uzma Khan, Yale SOM, 2005  
Michael Liersch, UCSD Psychology, 2007  
Elizabeth Keenan, UCSD, 2015  
Coby Morvinski, UCSD, 2015 (Chair)  
Charles Lin, UCSD Economics, 2015  
Kristen Duke, UCSD (Chair)  
Alicea Lieberman, UCSD (Chair)

*Conferences*

Program committee for: SCP, ACR, BDRM, SJDM  
Conference Chair: SCP 2017

***Reviewer***

Journal of Marketing Research  
Marketing Science  
Journal of Experimental Psychology: General  
Journal of Economic Psychology  
Journal of Consumer Research  
American Economic Review  
Journal of Consumer Psychology  
Memory and Cognition  
Psychology and Marketing  
Cognition  
Journal of Behavioral Decision Making  
Organizational Behavior and Human Decision Processes  
Psychological Science  
Journal of Personality and Social Psychology  
Management Science  
Journal of Economic Behavior and Organizations  
Science

***Member***

Association for Consumer Research  
Association for Consumer Psychology  
Society for Judgment and Decision Making  
American Psychological Society  
American Marketing Association

---

***Teaching Experience***

Marketing Management (MBA, Executive)  
Analytics in the wild (MBA, Executive)  
Consumer Behavior (MBA, Executive)  
Market Research (MBA, Executive)  
Social Psychology (teaching fellow, Harvard)  
E-Commerce Strategy (Executive)  
Data Driven Decision Making (Executive)  
Customized Executive Programs  
Pricing (Executive)  
Lab to Market (MBA, Executive)  
Intro to Business (Graduate)  
Branding (Executive)

***Consulting and Executive Teaching Experience***

Electronic Arts, HP Inc., Fiverr, Illumina, AAA, USAI, Cubic Corporation, Zimmer Dental, Life Technologies / Thermo Fisher, Intuit, WellBeat, Keiser Permanente, HP Software, Sony Entertainment, Applied Biosystems, Kumbaya App, Joyned, Marble, Themis-Tech.

# **APPENDIX B**

## **PRIOR TESTIMONY**

**Prior Testimony**

*Town of Apple Valley v. Apple Valley Ranchos Water Company*, Case No. CIV-DS-1600180, California Superior Court, San Bernardino. Retained by defendant. Deposed.

*Arechiga v. Kellwood Company/Vince LLC*, Case No. BC500988, Superior Court of California, County of Los Angeles. Retained by defendant. Deposed.

*San Diego County Credit Union v. Citizens Equity First Credit Union*, Case No. 3:18-CV-00967- GPC-MSB, United States District Court, Southern District of California. Retained by defendant. Deposed & court testimony.

*Yamagata v. Reckitt Benckiser LLC*, Case No. 3:17-cv-03529-VC, United States District Court, Northern District of California. Retained by defendant. Deposed.

*Warner Records, Inc., et al. v. Charter Communications, Inc.*, Case No. 1:19-cv-00874, United States District Court, District of Colorado. Retained by plaintiffs. Report submitted. Deposed.

*BBK Tobacco & Foods, LLP, an Arizona, limited liability partnership, d/b/a HBI International, v. Central Coast Agriculture, Inc., a Delaware corporation*, Case No. CV-19-05216-PHX-MTL, United States District Court, District of Arizona. Retained by plaintiff. Report submitted. Deposed.



# **APPENDIX C**

## **MATERIALS RELIED UPON**

## Materials Relied Upon

### Legal Documents

Order Denying Motion to Dismiss, *Chasom Brown et al., Plaintiffs, v. Google LLC, Defendant*, United States District Court, Northern District of California – Oakland Division, No. 5:20-cv-03664-YGR, March 12, 2021

Third Amended Complaint, *Chasom Brown, et al., Plaintiffs, v. Google LLC, Defendant*, United States District Court, Northern District of California – Oakland Division, No. 5:20-cv-03664-YGR, February 3, 2022

Video-Recorded Deposition of Jeremy Davis, January 7, 2022

Videotaped Deposition of Chasom Brown, January 13, 2022

Videotaped Deposition of Christopher Castillo, February 8, 2022

Virtual Videoconference Video-Recorded Deposition of Monique Trujillo, February 11, 2022

Zoom Videotaped Deposition of William Byatt, December 20, 2021

### Bates-Stamped Documents

GOOG-CABR-04067825-7867

GOOG-CABR-05156497-6555

### Academic Literature

Acquisti, Alessandro and Jens Grossklags, “Privacy and Rationality in Individual Decision Making,” *IEEE Security & Privacy*, Vol. 3, No. 1, 2005, pp. 26-33

Athey, Susan, et al., “The Digital Privacy Paradox: Small Money, Small Costs, Small Talk,” *NBER Working Paper Series*, 2017, pp. 1-26

Ben-Shahar, Omri and Lior J. Strahilevitz, “Interpreting Contracts Via Surveys and Experiments,” *New York University Law Review*, Vol. 92, 2017, pp. 1753-1827

Diamond, Shari S., “Reference Guide on Survey Research,” in *Reference Manual on Scientific Evidence*, Third Edition, 2011, The National Academies Press, pp. 359-423

Khan, Romana, et al., “Dynamic Customer Management and the Value of One-to-One Marketing,” *Marketing Science*, Vol. 28, No. 6, 2009, pp. 1063-1079

Kotler, Philip and Gary Armstrong, *Principles of Marketing*, Seventeenth Edition, Pearson, 2018

Lau, Josephine, et al., “Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers,” *Proceedings of the ACM on Human-Computer Interaction*, Vol. 2, Issue CSCW, 2018, pp. 1-31

Lavrakas, Paul. J., *Encyclopedia of Survey Research Methods*, SAGE Publications, Inc., 2008

*Manual for Complex Litigation*, Fourth Edition, Federal Judicial Center, 2004

Miller, Jeff, “Online Marketing Research,” in *The Handbook of Marketing Research*, Grover, Rajiv and Marco Vriens, eds., Sage Publications, 2006, pp. 110-131

Morales, Andrea C., et al., “Keeping it Real in Experimental Research — Understanding When, Where, and How to Enhance Realism and Measure Consumer Behavior,” *Journal of Consumer Research*, Vol. 44, No. 2, 2017, pp. 465-476

Sawyer, Alan G., “Demand Artifacts in Laboratory Experiments in Consumer Research,” *Journal of Consumer Research*, Vol. 1, No. 4, 1975, pp. 20-30

Tucker, Catherine E., “Social Networks, Personalized Advertising, and Privacy Controls,” *Journal of Marketing Research*, Vol. LI, 2014, pp. 546-562

### Other Publicly Available Sources

“About the User-ID Feature,” *Google Analytics Help*, available at <[https://support.google.com/analytics/answer/3123662?hl=en&ref\\_topic=3123660](https://support.google.com/analytics/answer/3123662?hl=en&ref_topic=3123660)>, accessed on March 18, 2022

“Browse in Private,” *Google*, available at <<https://support.google.com/chrome/answer/95464?hl=en>>, accessed on March 18, 2022

“Browser Market Share United States of America, 2009-2022,” *StatCounter*, available at <<https://gs.statcounter.com/browser-market-share/all/united-states-of-america/#yearly-2009-2022>>, accessed on March 18, 2022

“Browser Market Share Worldwide,” *StatCounter*, available at <<https://gs.statcounter.com/browser-market-share#yearly-2009-2022>>, accessed on March 18, 2022

“Chrome Privacy Notice,” May 20, 2020, *Google*, available at <<https://www.google.com/chrome/privacy/archive/20200520/>>

## Materials Relied Upon

- “Chrome Privacy Notice” (Desktop), May 20, 2020, available at <https://web.archive.org/web/20200521033250/https://www.google.com/chrome/privacy/>
- “Chrome Privacy Notice” (Mobile), May 20, 2020, available at <https://web.archive.org/web/20200521033250/https://www.google.com/chrome/privacy/>
- “Common Myths about Private Browsing,” *Mozilla*, available at [https://support.mozilla.org/en-US/kb/common-myths-about-private-browsing?as=u&utm\\_source=inproduct](https://support.mozilla.org/en-US/kb/common-myths-about-private-browsing?as=u&utm_source=inproduct), accessed on January 13, 2022
- “Desktop Browser Market Share United States of America, 2016-2022,” *StatCounter*, available at <https://gs.statcounter.com/browser-market-share/desktop/united-states-of-america/#yearly-2016-2022>, accessed on March 18, 2022
- “Desktop Browser Market Share Worldwide, 2009-2022,” *StatCounter*, available at <https://gs.statcounter.com/browser-market-share/desktop/worldwide/#yearly-2009-2022>, accessed on March 18, 2022
- “Desktop Operating System Market Share Worldwide, 2009-2022,” *StatCounter*, available at <https://gs.statcounter.com/os-market-share/desktop/worldwide/#yearly-2009-2022>, accessed on March 18, 2022
- “Find & Control Your Web & App Activity,” *Google*, available at <https://support.google.com/websearch/answer/54068?hl=en&co=GENIE.Platform%3DDesktop>, accessed on March 29, 2022
- “Google Chrome - Home,” *Google*, available at <https://www.google.com/chrome/>, accessed on March 18, 2022
- “Google Privacy Policy,” March 31, 2020, *Google*, available at <https://policies.google.com/privacy/archive/20200331?hl=en-US>
- “Google Privacy Policy” (Desktop), March 31, 2020, available at <https://web.archive.org/web/20200331221438/https://policies.google.com/privacy?hl=en-US>
- “Google Privacy Policy” (Mobile), March 31, 2020, available at <https://web.archive.org/web/20200331221438/https://policies.google.com/privacy?hl=en-US>
- “How Private Browsing Works in Chrome,” *Google*, available at [https://support.google.com/chrome/answer/7440301?hl=en&ref\\_topic=9845306](https://support.google.com/chrome/answer/7440301?hl=en&ref_topic=9845306), accessed on March 18, 2022
- “How Private Browsing Works in Chrome” (Desktop), May 26, 2020, *Google*, available at <https://web.archive.org/web/20200526023242/https://support.google.com/chrome/answer/7440301>
- “How Private Browsing Works in Chrome” (Mobile), July 6, 2020, *Google*, available at <https://web.archive.org/web/20200706003245/https://support.google.com/chrome/answer/7440301?co=GENIE.Platform%3DiOS&oco=1>
- “M83 Chrome Enterprise Release Notes,” May 19, 2020, *Chrome Enterprise*, available at <https://support.google.com/chrome/a/answer/10314655#83>
- “Mobile Browser Market Share United States Of America, 2016-2022,” *StatCounter*, available at <https://gs.statcounter.com/browser-market-share/mobile/united-states-of-america/#yearly-2016-2022>, accessed on March 18, 2022
- “Private Browsing in Firefox for iOS,” *Mozilla*, available at <https://support.mozilla.org/en-US/kb/private-browsing-firefox-ios>, accessed on January 14, 2022
- C., Suresh, “How to Start Secret Mode and Add New Tab in Samsung Internet?,” March 17, 2022, *BrowserHow*, available at: <https://browserhow.com/how-to-start-secret-mode-and-add-new-tab-in-samsung-internet/>, accessed on April 5, 2022
- Klein, Matt, “How to Enable Private Browsing on Any Web Browser,” July 5, 2017, *How-To Geek*, available at: <https://www.howtogeek.com/269265/how-to-enable-private-browsing-on-any-web-browser/#:~:text=To%20open%20a%20new%20InPrivate,return%20to%20regular%20browsing%20mode>, accessed on April 5, 2022
- Muchmore, Michael, “Chrome, Edge, Firefox, Opera, or Safari: Which Browser is Best?” May 20, 2021, *PCMag*, available at <https://www.pcmag.com/picks/chrome-edge-firefox-opera-or-safari-which-browser-is-best>, accessed on March 18, 2022
- Oppmann, Patrick, “In Digital World, We Trade Privacy for Convenience,” April 14, 2010, *CNN*, available at <http://www.cnn.com/2010/TECH/04/14/oppmann.off.the.grid/index.html>, accessed on March 29, 2022
- Pauzer, Holly, “71% of Consumers Prefer Personalized Ads,” *Adlucent*, available at <https://www.adlucent.com/resources/blog/71-of-consumers-prefer-personalized-ads/>, accessed on April 14, 2022
- Pilon, Anne, “Web Browser Survey: Firefox Still Ahead of Chrome,” January 6, 2012, *AYTM*, available at <https://aytm.com/blog/web-browser-survey/>, accessed on March 18, 2022
- Raine, Lee and Maeve Duggan, “Privacy and Information Sharing,” January 14, 2016, *Pew Research Center*, available at <https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/>, accessed on April 5, 2022

---

**Materials Relied Upon**

---

Screenshot of Chrome Incognito Splash Screen (Desktop), accessed on January 13, 2022

Screenshot of Chrome Incognito Splash Screen (Mobile), accessed on January 13, 2022

Screenshot of Firefox Private Browsing Splash Screen (Desktop), accessed on January 13, 2022

Screenshot of Firefox Private Browsing Splash Screen (Mobile), accessed on January 14, 2022

Screenshot of New Account Creation Agreement (Desktop), accessed on September 24, 2021

Screenshot of New Account Creation Agreement (Mobile), accessed on September 30, 2021

Screenshot of Safari Private Browsing Splash Screen (Desktop), accessed on January 13, 2022

Screenshot of Safari Private Browsing Splash Screen (Mobile), accessed on January 14, 2022

---

***Other***

---

Consumer Perceptions and Expectations Survey Data, fielded from March 16 to 21, 2022 ("2203704.xlsx")

Interpretation Survey Data, fielded from March 16 to 21, 2022 ("2203487.xlsx")

Likelihood of Use Survey Data, fielded from March 16 to 21, 2022 ("2203523.xlsx")

# **APPENDIX D**

## **PRETEST MODERATOR INSTRUMENT**

### Pretest Moderator Instrument

[Blind-to-the-purpose interviewer at the survey vendor conducts interview over the phone while respondent takes the survey online.]

Q0-1. Hello, can I please speak with [NAME]?

Q0-2A. **[IF THE RESPONDENT PICKS UP THE PHONE]** I am calling from [PANEL] regarding a phone interview that you scheduled with us. Is now still a good time?

- ☐ Yes
- ☐ No **[SCHEDULE CALLBACK]**

Q0-2B. **[IF SOMEONE PICKS UP THE PHONE WHO IS NOT THE RESPONDENT]** I am calling from [PANEL] regarding a phone interview that [NAME] scheduled with us. He/she agreed to offer his/her opinions. Is [NAME] available?

- ☐ Yes
- ☐ No **[SCHEDULE CALLBACK]**

I would like to let you know that this call may be monitored for quality assurance purposes. **[DO NOT WAIT FOR AN ANSWER, CONTINUE WITH THE SURVEY UNLESS THE RESPONDENT SAYS OTHERWISE.]**

Q0-3. [NAME], thank you for your time in taking this survey with us today. To start, are you on your computer or your mobile device right now?

- ☐ Yes
- ☐ No **[WAIT UNTIL THEY ARE ON A COMPUTER OR A MOBILE DEVICE]**

Q0-4. Thank you! In the email you received from us, there is a link to the website you need to go to. Please click on that link. **[IF NEEDED, REMIND RESPONDENT OF THE SENDER OF THE EMAIL, OR RESEND LINK].**

I will be on the phone with you the entire time while you are taking the survey. Please feel free to “think out loud” or bring up anything you would like while you are taking the survey. There is no correct or incorrect way to take this survey. Please be thorough in your response and take as much time as you need. We would like you to approach this exercise as realistically as possible.

Please also note that the first few questions are the same as the ones in the survey you took to qualify for this interview.

You can begin the survey whenever you are ready.

**[LET THE RESPONDENT TAKE THE SURVEY AND COMPLETE IT.]**

**[ASK THE FOLLOWING QUESTIONS AFTER THE RESPONDENT HAS FINISHED THE SURVEY.]**

Q1. Did you have any issues while taking the survey?

Q2. Did you think any questions were unclear? If so, which ones and why?

Q3. Did you think any answer options were unclear? If so, which ones and why?

Q4. Did you or did you not have any issues viewing the survey or images in the survey?

Q5. Did you think that the text guiding you through the survey was clear?

Q6. What do you think might be the purpose for conducting this survey?

Q7. What makes you think so?

Q8. Is there anything else you would like to say about the survey?

Thank you very much for your time. We greatly appreciate your help, and we will ensure that you get credit for taking this survey.



# **APPENDIX E**

## **PRETEST SUMMARY**

### Summary of Pre-Tests

Follow-up Question	No problems	Some problems	Total
Q1. Did you have any issues while taking the survey? <sup>[1]</sup>	27	3	30
Q2. Did you think any questions were unclear? If so, which ones and why? <sup>[2]</sup>	28	2	30
Q3. Did you think any answer options were unclear? If so, which ones and why? <sup>[3]</sup>	28	2	30
Q4. Did you or did you not have any issues viewing the survey or images in the survey? <sup>[4][5]</sup>	26	4	30
Q5. Did you think that the text guiding you through the survey was clear? <sup>[6]</sup>	28	2	30

#### Notes:

[1] One respondent was worried that they were unable to reach the end of the survey. Another respondent mentioned having an issue with the zoom in feature. A third respondent said that the survey took a long time to load and that it was hard to navigate the screen.

[2] One respondent had issues with the hyperlink on the private browsing splash screen. A second respondent had a question about what was meant by Google receiving information.

[3] One respondent wanted a clarification on whether the question was asking about temporary or permanent storage of cookies. The same respondent who asked about what was meant by Google receiving information in Q2 asked what was meant by “receive” again.

[4] One respondent had trouble loading the first image. The other three respondents who ran into some problems mentioned confusion with the zoom functionality.

[5] One respondent indicated that some of the image text was too small. Since this respondent did not make this comment when answering Q4, this respondent was not counted here.

[6] One respondent mentioned issues reading the text on the Incognito screen because of the dark background, while another respondent mentioned issues reading the text on the Incognito screen because of the small font size.

#### Source:

Pretest notes.

**APPENDIX F.1**

**CONSUMER PERCEPTIONS  
AND EXPECTATIONS  
SURVEY INSTRUMENT**

**Consumer Perceptions and Expectations Survey Instrument  
Survey Programmer Instructions**

**LEGEND:**

**[PROGRAMMER NOTES IN BOLD CAPS AND BRACKETS]**

*Notes to respondent in italics*

**FORMAT:** The survey consists of the following sections:

<b>Introduction &amp; Screening</b> (questions labeled QS)
<b>Main Survey Questions</b> (questions labeled Q)
<b>Follow-Up Questions</b> (questions labeled QF)

**Overview**

**[NATIONAL 18+ SAMPLE]**

**[PANEL MEMBERS SHOULD BE MATCHED TO THE CENSUS ON AGE, GENDER, AND REGION. THAT IS, THE SCREENER SHOULD BE APPLIED TO A SAMPLE REPRESENTATIVE OF THE GENERAL POPULATION IN THE UNITED STATES SO THAT THE FINAL SAMPLE IS REPRESENTATIVE OF THE TARGET POPULATION FOR THE SURVEY (BASED ON ACTUAL QUALIFICATION).]**

**[TARGET 500 COMPLETES]**

**[DISABLE THE BROWSER’S “BACK” BUTTON AND DO NOT SHOW A “BACK” BUTTON WITHIN THE SURVEY]**

**[FORCE RESPONSES TO ALL QUESTIONS]**

**[NO SURVEY TITLE AND NO QUESTION NUMBER TO BE DISPLAYED TO RESPONDENTS]**

**[DIGITAL FINGERPRINTING SHOULD BE USED TO AVOID REPEAT PARTICIPATION. DO NOT INVITE RESPONDENTS WHO WERE INVITED TO TAKE OTHER SURVEYS IN THIS MATTER]**

**[TEXT FOR TERMINATES: “THANK YOU FOR YOUR INTEREST IN OUR STUDY. WE ARE NO LONGER LOOKING FOR PEOPLE WHO MATCH YOUR CHARACTERISTICS. WE APPRECIATE YOUR TIME.”]**

**Introduction and Screening**

QS0. Please enter the code exactly as it appears in the image below and then click “Continue” to continue.

**[INSERT CAPTCHA; TERMINATE IF NOT CORRECT AFTER FOUR TRIES]**

**[IF NO RESPONSE IS SELECTED OR CAPTCHA CODE IS INCORRECT, DISPLAY TEXT  
“PLEASE ENTER THE CORRECT CODE.”]**

**[NEXT PAGE]**

QS1. Thank you for participating in our study. Your opinions are very important to us. If you don't know an answer to a question or if you don't have an opinion, please don't guess. Simply indicate this in your response by selecting the “Don't know / Unsure” option or the “I don't feel I have enough information to answer this question” option. There are no right or wrong answers.

Your answers will be kept in strict confidence and the results of this study will not be used to try to sell you anything. Trademarks and logos are all the intellectual property of their respective owners.

If you wear glasses or corrective lenses when using a desktop computer, laptop computer, mobile phone, or tablet, please wear them throughout the survey.

Please do not use the “Back” button of your browser while taking the survey. This survey will take less than 15 minutes of your time. When you are ready to get started, please select the “Continue” button.

**[NEXT PAGE]**

QS2. What is your age? *(Select only one option)*

**[ROTATE ORDER, AS IS AND REVERSE; KEEP “PREFER NOT TO ANSWER” LAST]**

- ☐ Under 18 **[TERMINATE]**
- ☐ 18 - 29
- ☐ 30 - 39
- ☐ 40 - 49
- ☐ 50 - 59
- ☐ 60 or older
- ☐ Prefer not to answer **[ANCHOR LAST; TERMINATE]**

**[TERMINATE IF AGE DOES NOT MATCH THE VALUE PASSED BY PANEL PROVIDER]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QS3. Are you...? *(Select only one option)*

**[ROTATE ORDER, AS IS AND REVERSE; KEEP “OTHER” AND “PREFER NOT TO ANSWER” LAST]**

- ☐ Male
- ☐ Female
- ☐ Other **[ANCHOR SECOND TO LAST]**
- ☐ Prefer not to answer **[ANCHOR LAST; TERMINATE]**

**[TERMINATE IF GENDER DOES NOT MATCH THE VALUES PASSED BY PANEL PROVIDER ONLY IF “MALE” OR “FEMALE” IS SELECTED]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QS4. In which state do you live? *(Select only one option)*

**[DROP DOWN MENU OF 50 STATES + DISTRICT OF COLUMBIA; HIDDEN VARIABLE FOR REGION; DETERMINE US CENSUS REGION BASED ON STATE SELECTED. ADD “PREFER NOT TO ANSWER” AND “DON’T KNOW / UNSURE” OPTIONS BELOW DROP DOWN MENU]**

- ☐ Prefer not to answer **[ANCHOR SECOND TO LAST; TERMINATE]**
- ☐ Don’t know / Unsure **[ANCHOR LAST; TERMINATE]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT EITHER A STATE, PREFER NOT TO ANSWER, OR DON’T KNOW / UNSURE.”]**

**[NEXT PAGE]**

QS5. Have you or any member of your household ever worked for any of the following types of companies? *(Select all that apply)*

**[RANDOMIZE LIST; KEEP “NONE OF THE ABOVE” LAST]**

- ☐ A technology company or technology consultancy
- ☐ A law firm, legal services organization, or court **[TERMINATE]**
- ☐ A marketing, market research, or advertising agency
- ☐ An academic institution
- ☐ A construction company
- ☐ A clothing retailer
- ☐ A real estate agency
- ☐ A car dealership
- ☐ A fitness center
- ☐ A healthcare provider or medical office
- ☐ None of the above **[ANCHOR LAST; EXCLUSIVE]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT THE RELEVANT COMPANY TYPE(S) OR NONE OF THE ABOVE.”]**

**[NEXT PAGE]**

QS6. This question is to check your attention. Please select “South” from the answer options below.  
(*Select only one option*)

**[RANDOMIZE ORDER; KEEP “NONE OF THE ABOVE” AND “DON’T KNOW / UNSURE” LAST]**

- ☐ North
- ☐ East
- ☐ South
- ☐ West
- ☐ None of the above **[ANCHOR SECOND TO LAST]**
- ☐ Don’t know / Unsure **[ANCHOR LAST]**

**[TERMINATE IF “SOUTH” IS NOT SELECTED]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QS7. Thinking about the device(s) you use to browse the internet (such as your phone, your personal laptop, or your office computer), which internet browser(s) do you currently use? (*Select all that apply*)

**[RANDOMIZE LIST; KEEP “OTHER” AND “DON’T KNOW / UNSURE” LAST]**

- ☐ Internet Explorer
- ☐ Microsoft Edge
- ☐ Safari
- ☐ Brave
- ☐ Google Chrome
- ☐ Mozilla Firefox
- ☐ Opera
- ☐ DuckDuckGo
- ☐ Odeon **[TERMINATE]**
- ☐ Other (*Please specify*) \_\_\_\_\_ **[ANCHOR SECOND TO LAST]**
- ☐ Don’t know / Unsure **[ANCHOR LAST; EXCLUSIVE]**

**[TERMINATE IF ANY COMBINATION OF ANSWER OPTIONS CONTAINING “ODEON” IS SELECTED]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT EITHER THE INTERNET BROWSER(S) YOU USE OR DON’T KNOW / UNSURE.”]**

**[NEXT PAGE]**



QS8. In the past six months, which of the following features, if any, have you used on your internet browser(s)? (*Select all that apply*)

[RANDOMIZE LIST; KEEP “OTHER” AND “DON’T KNOW / UNSURE” LAST]

- ☐ Private browsing mode
- ☐ Bookmarks
- ☐ Website translator
- ☐ Customized home page
- ☐ Screenshot tool
- ☐ Dark mode for visual display
- ☐ Other (*Please specify*) \_\_\_\_\_ [ANCHOR SECOND TO LAST]
- ☒ Don’t know / Unsure [ANCHOR LAST; EXCLUSIVE]

[TERMINATE IF “PRIVATE BROWSING MODE” IS NOT SELECTED]

[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT THE FEATURES YOU USED ON YOUR INTERNET BROWSER(S) OR SELECT DON’T KNOW / UNSURE.”]

[NEXT PAGE]

## Main Questionnaire

[ASSIGN RESPONDENT TO CELLS BASED ON THE FOLLOWING:

FIRST, ASSIGN RESPONDENT TO BROWSER GROUP:

- AMONG “GOOGLE CHROME”, “SAFARI,” AND “MOZILLA FIREFOX” IN QS7, IF RESPONDENT SELECTED ONLY “GOOGLE CHROME,” ASSIGN TO “CHROME” GROUP.
- AMONG “GOOGLE CHROME”, “SAFARI,” AND “MOZILLA FIREFOX” IN QS7, IF RESPONDENT SELECTED ONLY “SAFARI,” ASSIGN TO “SAFARI” GROUP.
- AMONG “GOOGLE CHROME”, “SAFARI,” AND “MOZILLA FIREFOX” IN QS7, IF RESPONDENT SELECTED ONLY “MOZILLA FIREFOX,” ASSIGN TO “FIREFOX” GROUP.
- AMONG “GOOGLE CHROME”, “SAFARI,” AND “MOZILLA FIREFOX” IN QS7, IF RESPONDENT SELECTED MORE THAN ONE OPTIONS, RANDOMIZE BROWSER GROUP AMONG THE SELECTED OPTIONS.
- AMONG “GOOGLE CHROME”, “SAFARI,” AND “MOZILLA FIREFOX” IN QS7, IF RESPONDENT DID NOT SELECT ANY OPTION, RANDOMIZE BROWSER GROUP.

SECOND ASSIGN RESPONDENT TO MOBILE OR DESKTOP VERSION:

- DETECT DEVICE RESPONDENT IS USING.
- IF RESPONDENT IS USING A DESKTOP COMPUTER, LAPTOP COMPUTER, OR TABLET, PRESENT DESKTOP VERSION.
- IF RESPONDENT IS USING A MOBILE DEVICE, PRESENT MOBILE VERSION.

		Mobile or Desktop Version	Completes Breakdown 500 completes
Browser Group	Chrome	Desktop	Minimum 200 completes (with minimum 80 completes in desktop version)
		Mobile	
	Safari	Desktop	Minimum 50 completes
		Mobile	
	Firefox	Desktop	Minimum 50 completes
		Mobile	

Q0. Based on your answers to the previous questions, you have qualified for this survey.

[NEXT PAGE]

**[IN THE BRACKETS IN Q1, DISPLAY “TWO IMAGES” OR “THESE IMAGES” IF RESPONDENT IS ASSIGNED TO “CHROME” OR “FIREFOX” GROUP AND “AN IMAGE” OR “THIS IMAGE” IF RESPONDENT IS ASSIGNED TO “SAFARI” GROUP]**

- Q1. This survey is about what you expect while in private browsing mode. You will first see [two images / an image]. After, you will be asked to answer a few questions. You will be able to view [these images / this image] again as you answer the questions.

Please do not use your browser’s “Back” button.

If you don’t know an answer to a question or if you don’t have an opinion, please don’t guess. Simply indicate this in your response by selecting the “Don’t know / Unsure” option or the “I don’t feel I have enough information to answer this question” option. There are no right or wrong answers.

**[NEXT PAGE]**

- Q2. Imagine that you decide to open [MODE NAME] window and see the screen below.  
[INSTRUCTIONS]

Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

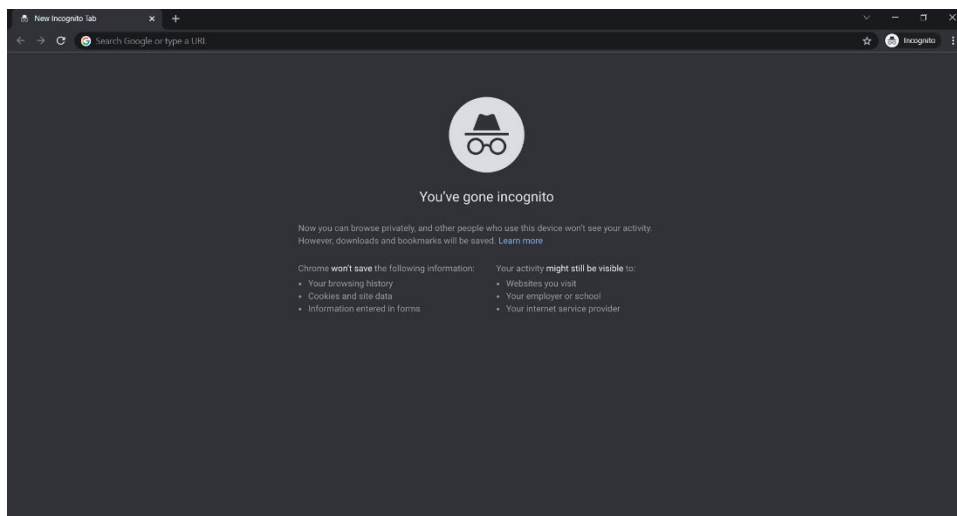
**[PIPE INTO “MODE NAME” “an Incognito” IF RESPONDENT IS ASSIGNED TO “CHROME” GROUP OR “a Private Browsing” IF RESPONDENT IS ASSIGNED TO “SAFARI” OR “FIREFOX” GROUPS]**

**[PIPE INTO “INSTRUCTIONS” “Hyperlinks have been enabled in this image.” IF RESPONDENT IS ASSIGNED TO “CHROME” OR “FIREFOX” GROUPS OR “Hyperlinks and any other clickable elements in this image have been disabled.” IF RESPONDENT IS ASSIGNED TO “SAFARI” GROUP]**

**[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]**

**[DISPLAY PRIVATE BROWSING MODE SPLASH SCREEN IMAGE]**

**[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 30 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 30. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]**



**[CREATE HYPERLINK TO “LEARN MORE” ON THE IMAGE AND RECORD WHETHER OR NOT RESPONDENT CLICKS ON IT.**

- **IF RESPONDENT CLICKS ON “LEARN MORE” BEFORE THE 30-SECOND TIMER EXPIRES, PRESENT A POP UP WITH THE FOLLOWING MESSAGE, “YOU WILL BE TAKEN TO THE NEXT PAGE IN [X] SECONDS.” WHERE X IS A TIMER THAT MIRRORS THE NUMBER OF SECONDS REMAINING IN THE 30-SECOND TIMER FOR THE PAGE. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP. TAKE RESPONDENT TO Q3 WHEN THE TIMER EXPIRES.**
- **IF RESPONDENT CLICKS ON “LEARN MORE” AFTER THE 30-SECOND TIMER EXPIRES, TAKE RESPONDENT TO Q3.**

**CLICKING THE “CONTINUE” BUTTON AFTER THE TIMER EXPIRES WILL ALSO TAKE RESPONDENT TO Q3]**

**[“SAFARI” GROUP WILL NOT HAVE A HYPERLINK AND Q3. RESPONDENT WILL GO TO Q4 AFTER Q2]**

**[NEXT PAGE]**

Q3. You will now see the following screen that would appear if you clicked “Learn more” on the previous page. Hyperlinks and any other clickable elements in this image have been disabled.

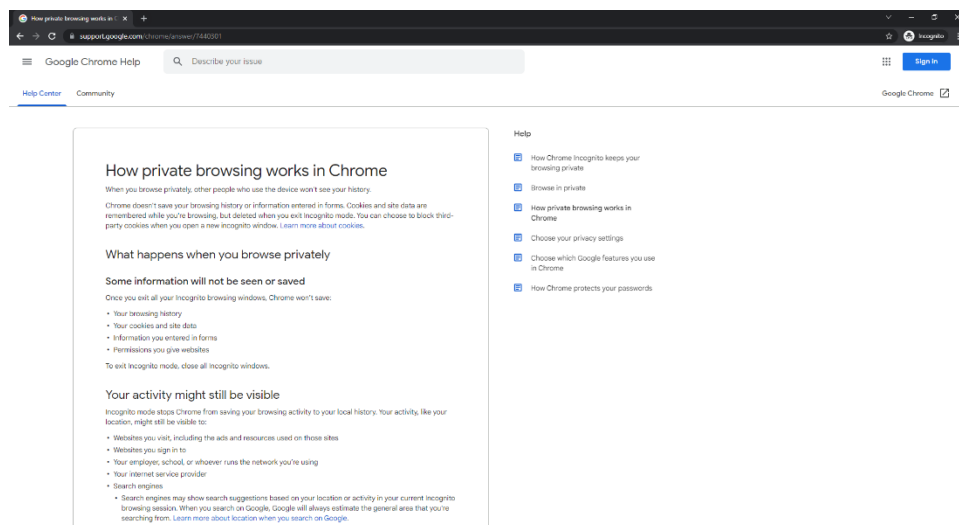
Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]

[DISPLAY “LEARN MORE” PAGE IMAGE]

[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 30 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 30. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]

[PROGRAM THE “LEARN MORE” PAGE IMAGE TO BE SCROLLABLE WITHIN THE BROWSER WINDOW FRAME]



[NEXT PAGE]

[PRESENT ALL IMAGES THAT THE RESPONDENT REVIEWED AS THUMBNAIL IMAGES AT THE BOTTOM OF THE PAGE FOR Q4-Q6]

[AT THE TOP OF EACH PAGE FOR Q4-Q6, DISPLAY THE FOLLOWING TEXT IF RESPONDENT WAS ASSIGNED TO “SAFARI” GROUP: “(The thumbnail contains the image that you have viewed earlier. You can click on the thumbnail to see the enlarged version of this image.)”. DISPLAY THE FOLLOWING TEXT IF RESPONDENT WAS ASSIGNED TO “CHROME” OR

**“FIREFOX” GROUPS:** “(The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.)”]

**[FOR Q4-Q6, PIPE INTO “MODE NAME” “Incognito mode” IF RESPONDENT IS ASSIGNED TO “CHROME” GROUP OR “Private Browsing mode” IF RESPONDENT IS ASSIGNED TO “SAFARI” OR “FIREFOX” GROUPS]**

**[IN Q4-Q6, IF RESPONDENT HOVERS OVER “IP ADDRESS” IN THE QUESTION, DISPLAY THE FOLLOWING TEXT, “Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. An IP address can often be used to identify the location from which a device is connecting to the Internet.”]**

**[IN Q4-Q6, IF RESPONDENT HOVERS OVER “URLS OF THE SITES YOU VISIT” IN THE QUESTION, DISPLAY THE FOLLOWING TEXT, “The web addresses of the webpages you visited using the browser.”]**

**[IN Q4-Q6, IF RESPONDENT HOVERS OVER “COOKIES” IN THE QUESTION, DISPLAY THE FOLLOWING TEXT, “A small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information.”]**

**[RANDOMIZE ORDER SHOWN OF Q4-Q6]**

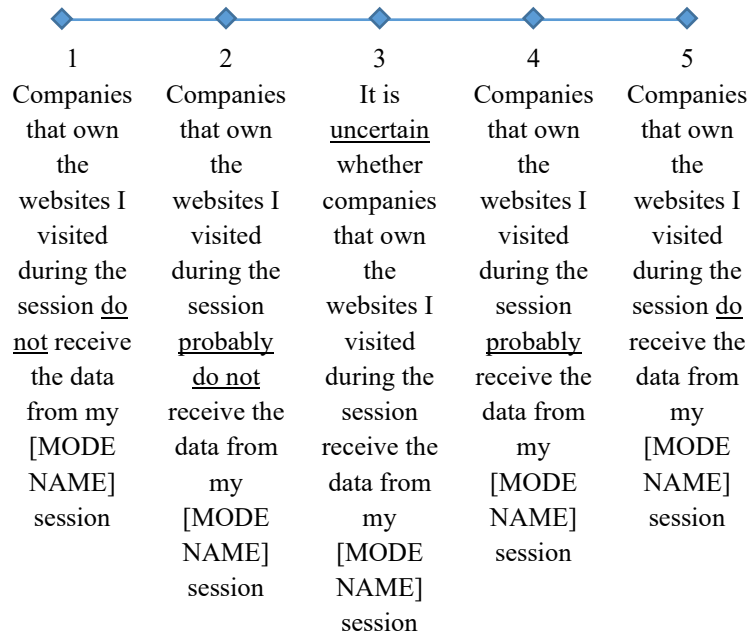
**[FOR Q4-Q6, RANDOMIZE ORDER OF FIRST 5 OPTIONS BETWEEN 1-2-3-4-5 OR 5-4-3-2-1, NO STARTING POINT. DO NOT SHOW NUMBERS ON SCALE TO RESPONDENTS. MAINTAIN SAME ORDER OF OPTIONS ACROSS Q4-Q6]**

**[FOR Q4-Q6, IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

- Q4. While in [MODE NAME] mode, do the companies that own the websites you visited during the session receive or not receive the data from your [MODE NAME] session (such as IP address, URLs of the sites you visit, and cookies)?

Please base your answer on the screens you reviewed.

*(Select a point on the scale. If you do not have enough information, please select “I don’t feel I have enough information to answer this question”)*



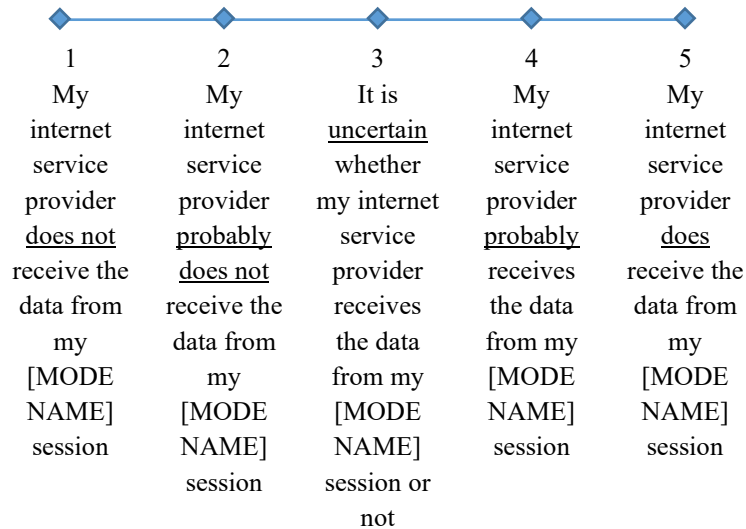
Ⓢ I don’t feel I have enough information to answer this question [EXCLUSIVE]

[NEXT PAGE]

- Q5. While in [MODE NAME] mode, does your internet service provider receive or not receive the data from your [MODE NAME] session (such as IP address, URLs of the sites you visit, and cookies)?

Please base your answer on the screens you reviewed.

*(Select a point on the scale. If you do not have enough information, please select “I don’t feel I have enough information to answer this question”)*



⊙ I don’t feel I have enough information to answer this question [EXCLUSIVE]

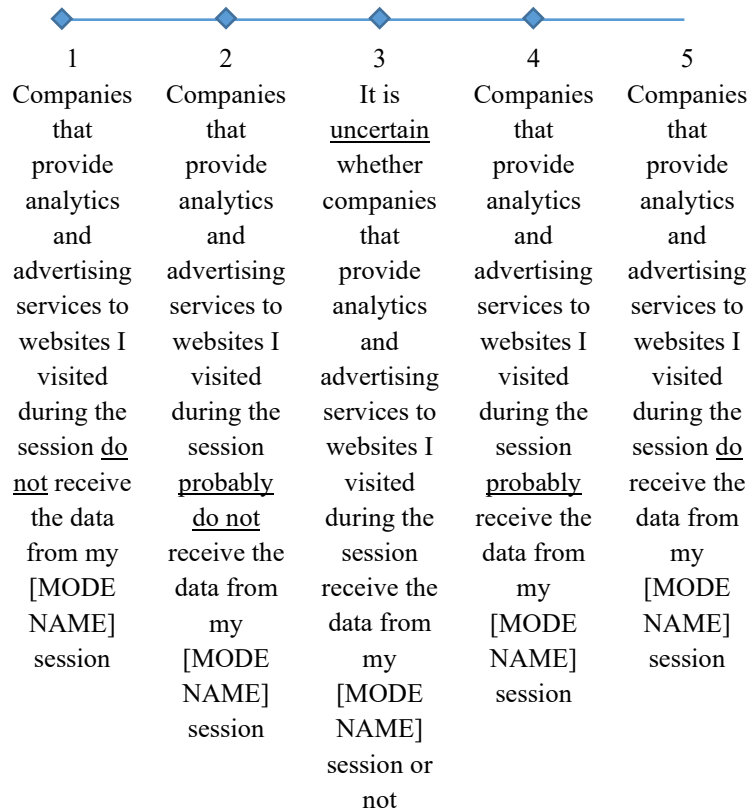
[NEXT PAGE]



- Q6. While in [MODE NAME] mode, do companies that provide analytics and advertising services to websites you visited during the session receive or not receive the data from your [MODE NAME] session (such as IP address, URLs of the sites you visit, and cookies)?

Please base your answer on the screens you reviewed.

*(Select a point on the scale. If you do not have enough information, please select “I don’t feel I have enough information to answer this question”)*



Ⓒ I don’t feel I have enough information to answer this question [EXCLUSIVE]

[NEXT PAGE]

**Follow Up Questions**

**[IN THE BRACKETS IN QF1, DISPLAY “IMAGE” IF RESPONDENT REVIEWED ONE IMAGE AND “IMAGES” IF RESPONDENT REVIEWED MORE THAN ONE IMAGE]**

QF1. Were you or were you not able to view the [images / image] clearly to answer the questions asked in this survey? *(Select only one option)*

**[RANDOMIZE ORDER; KEEP “DON’T KNOW / UNSURE” LAST]**

- ☐ I was able to view the [images / image] clearly to answer the questions asked in this survey
- ☐ I was not able to view the [images / image] clearly to answer the questions asked in this survey
- ☐ Don’t know / Unsure **[ANCHOR LAST]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QF2. Prior to this survey, were you or were you not aware of any lawsuits related to private browsing mode? *(Select only one option)*

**[USE THE SAME ORDER OF HAVE/HAVE NOT ANSWERS AS IN QF1]**

- ☐ I was aware of at least one lawsuit related to private browsing mode
- ☐ I was not aware of any lawsuit related to private browsing mode **[SKIP TO QF4]**
- ☐ Don’t know / Unsure **[ANCHOR LAST; SKIP TO QF4]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QF3. You indicated that you were aware of at least one lawsuit regarding private browsing mode. Please describe the lawsuit(s) you were aware of: *(Please type in your response. If you do not know the answer or are unsure, please select “Don’t know / Unsure”)*

**[OPEN-ENDED TEXT BOX, LIMITING TO 1000 CHARACTERS]**

**[REQUIRE AT LEAST 4 CHARACTERS; SHOW ERROR “Please be thorough in your response.” IF ENTRY IS LESS THAN 4 CHARACTERS]**

- ☐ Don’t know / Unsure **[EXCLUSIVE]**

**[IF NO RESPONSE IS PROVIDED, DISPLAY TEXT “PLEASE TYPE A RESPONSE OR SELECT DON’T KNOW / UNSURE.”]**

**[NEXT PAGE]**

QF4. In the past three months, have you or have you not taken any other survey related to private browsing mode? (*Select only one option*)

**[USE THE SAME ORDER OF HAVE/HAVE NOT ANSWERS AS IN QF1]**

- ☐ I have taken a survey related to private browsing mode
- ☐ I have not taken a survey related to private browsing mode
- ☐ Don't know / Unsure **[ANCHOR LAST]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT "PLEASE SELECT AN ANSWER."]**

**[GO TO PANEL THANK YOU PAGE]**

# **APPENDIX F.2**

## **INTERPRETATION SURVEY INSTRUMENT**

## Interpretation Survey Instrument Survey Programmer Instructions

### **LEGEND:**

**[PROGRAMMER NOTES IN BOLD CAPS AND BRACKETS]**

*Notes to respondent in italics*

**FORMAT:** The survey consists of the following sections:

<b>Introduction &amp; Screening</b> (questions labeled QS)
<b>Main Survey Questions</b> (questions labeled Q)
<b>Follow-Up Questions</b> (questions labeled QF)

### **Overview**

**[NATIONAL 18+ SAMPLE]**

**[PANEL MEMBERS SHOULD BE MATCHED TO THE CENSUS ON AGE, GENDER, AND REGION. THAT IS, THE SCREENER SHOULD BE APPLIED TO A SAMPLE REPRESENTATIVE OF THE GENERAL POPULATION IN THE UNITED STATES SO THAT THE FINAL SAMPLE IS REPRESENTATIVE OF THE TARGET POPULATION FOR THE SURVEY (BASED ON ACTUAL QUALIFICATION).]**

**[TARGET 1000 COMPLETES]**

**[DISABLE THE BROWSER’S “BACK” BUTTON AND DO NOT SHOW A “BACK” BUTTON WITHIN THE SURVEY]**

**[FORCE RESPONSES TO ALL QUESTIONS]**

**[NO SURVEY TITLE AND NO QUESTION NUMBER TO BE DISPLAYED TO RESPONDENTS]**

**[DIGITAL FINGERPRINTING SHOULD BE USED TO AVOID REPEAT PARTICIPATION. DO NOT INVITE RESPONDENTS WHO WERE INVITED TO TAKE OTHER SURVEYS IN THIS MATTER]**

**[TEXT FOR TERMINATES: “THANK YOU FOR YOUR INTEREST IN OUR STUDY. WE ARE NO LONGER LOOKING FOR PEOPLE WHO MATCH YOUR CHARACTERISTICS. WE APPRECIATE YOUR TIME.”]**

### **Introduction and Screening**

QS0. Please enter the code exactly as it appears in the image below and then click “Continue” to continue.

**[INSERT CAPTCHA; TERMINATE IF NOT CORRECT AFTER FOUR TRIES]**

**[IF NO RESPONSE IS SELECTED OR CAPTCHA CODE IS INCORRECT, DISPLAY TEXT  
“PLEASE ENTER THE CORRECT CODE.”]**

**[NEXT PAGE]**

QS1. Thank you for participating in our study. Your opinions are very important to us. If you don't know an answer to a question or if you don't have an opinion, please don't guess. Simply indicate this in your response by selecting the “Don't know / Unsure” option or the “I don't feel I have enough information to answer this question” option. There are no right or wrong answers.

Your answers will be kept in strict confidence and the results of this study will not be used to try to sell you anything. Trademarks and logos are all the intellectual property of their respective owners.

If you wear glasses or corrective lenses when using a desktop computer, laptop computer, mobile phone, or tablet, please wear them throughout the survey.

Please do not use the “Back” button of your browser while taking the survey. This survey will take less than 15 minutes of your time. When you are ready to get started, please select the “Continue” button.

**[NEXT PAGE]**

QS2. What is your age? *(Select only one option)*

**[ROTATE ORDER, AS IS AND REVERSE; KEEP “PREFER NOT TO ANSWER” LAST]**

- ☐ Under 18 **[TERMINATE]**
- ☐ 18 - 29
- ☐ 30 - 39
- ☐ 40 - 49
- ☐ 50 - 59
- ☐ 60 or older
- ☐ Prefer not to answer **[ANCHOR LAST; TERMINATE]**

**[TERMINATE IF AGE DOES NOT MATCH THE VALUE PASSED BY PANEL PROVIDER]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QS3. Are you...? *(Select only one option)*

**[ROTATE ORDER, AS IS AND REVERSE; KEEP “OTHER” AND “PREFER NOT TO ANSWER” LAST]**

- ☐ Male
- ☐ Female
- ☐ Other **[ANCHOR SECOND TO LAST]**
- ☐ Prefer not to answer **[ANCHOR LAST; TERMINATE]**

**[TERMINATE IF GENDER DOES NOT MATCH THE VALUES PASSED BY PANEL PROVIDER ONLY IF “MALE” OR “FEMALE” IS SELECTED]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QS4. In which state do you live? *(Select only one option)*

**[DROP DOWN MENU OF 50 STATES + DISTRICT OF COLUMBIA; HIDDEN VARIABLE FOR REGION; DETERMINE US CENSUS REGION BASED ON STATE SELECTED. ADD “PREFER NOT TO ANSWER” AND “DON’T KNOW / UNSURE” OPTIONS BELOW DROP DOWN MENU]**

- ☐ Prefer not to answer **[ANCHOR SECOND TO LAST; TERMINATE]**
- ☐ Don’t know / Unsure **[ANCHOR LAST; TERMINATE]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT EITHER A STATE, PREFER NOT TO ANSWER, OR DON’T KNOW / UNSURE.”]**

**[NEXT PAGE]**

QS5. Have you or any member of your household ever worked for any of the following types of companies? *(Select all that apply)*

**[RANDOMIZE LIST; KEEP “NONE OF THE ABOVE” LAST]**

- ☐ A technology company or technology consultancy
- ☐ A law firm, legal services organization, or court **[TERMINATE]**
- ☐ A marketing, market research, or advertising agency
- ☐ An academic institution
- ☐ A construction company
- ☐ A clothing retailer
- ☐ A real estate agency
- ☐ A car dealership
- ☐ A fitness center
- ☐ A healthcare provider or medical office
- ☐ None of the above **[ANCHOR LAST; EXCLUSIVE]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT THE RELEVANT COMPANY TYPE(S) OR NONE OF THE ABOVE.”]**

**[NEXT PAGE]**

QS6. This question is to check your attention. Please select “South” from the answer options below.  
(*Select only one option*)

**[RANDOMIZE ORDER; KEEP “NONE OF THE ABOVE” AND “DON’T KNOW / UNSURE” LAST]**

- ☐ North
- ☐ East
- ☐ South
- ☐ West
- ☐ None of the above **[ANCHOR SECOND TO LAST]**
- ☐ Don’t know / Unsure **[ANCHOR LAST]**

**[TERMINATE IF “SOUTH” IS NOT SELECTED]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QS7. Thinking about the device(s) you use to browse the internet (such as your phone, your personal laptop, or your office computer), which internet browser(s) do you currently use? (*Select all that apply*)

**[RANDOMIZE LIST; KEEP “OTHER” AND “DON’T KNOW / UNSURE” LAST]**

- ☐ Internet Explorer
- ☐ Microsoft Edge
- ☐ Safari
- ☐ Brave
- ☐ Google Chrome
- ☐ Mozilla Firefox
- ☐ Opera
- ☐ DuckDuckGo
- ☐ Odeon **[TERMINATE]**
- ☐ Other (*Please specify*) \_\_\_\_\_ **[ANCHOR SECOND TO LAST]**
- ☐ Don’t know / Unsure **[ANCHOR LAST; EXCLUSIVE]**

**[TERMINATE IF ANY COMBINATION OF ANSWER OPTIONS CONTAINING “ODEON” IS SELECTED]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT EITHER THE INTERNET BROWSER(S) YOU USE OR DON’T KNOW / UNSURE.”]**

**[NEXT PAGE]**



QS8. In the past six months, which of the following features, if any, have you used on your internet browser(s)? (*Select all that apply*)

[RANDOMIZE LIST; KEEP “OTHER” AND “DON’T KNOW / UNSURE” LAST]

- ☐ Private browsing mode
- ☐ Bookmarks
- ☐ Website translator
- ☐ Customized home page
- ☐ Screenshot tool
- ☐ Dark mode for visual display
- ☐ Other (*Please specify*) \_\_\_\_\_ [ANCHOR SECOND TO LAST]
- ☒ Don’t know / Unsure [ANCHOR LAST; EXCLUSIVE]

[TERMINATE IF “PRIVATE BROWSING MODE” IS NOT SELECTED]

[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT THE FEATURES YOU USED ON YOUR INTERNET BROWSER(S) OR SELECT DON’T KNOW / UNSURE.”]

[NEXT PAGE]

## Main Questionnaire

[ASSIGN RESPONDENT TO CELLS BASED ON THE FOLLOWING:

FIRST, ASSIGN RESPONDENT TO GROUP:

- RANDOMIZE RESPONDENT TO “SPLASH SCREEN ONLY”, “SPLASH SCREEN WITH POLICIES (HIGHLIGHTED)”, “SPLASH SCREEN WITH NEW ACCOUNT CREATION AGREEMENT”, OR “SPLASH SCREEN WITH CONSENT BUMP AGREEMENT AND FAQ PAGE” GROUP.

SECOND, ASSIGN RESPONDENT TO MOBILE OR DESKTOP VERSION:

- DETECT DEVICE RESPONDENT IS USING.
- IF RESPONDENT IS USING A DESKTOP COMPUTER, LAPTOP COMPUTER, OR TABLET, PRESENT DESKTOP VERSION.
- IF RESPONDENT IS USING A MOBILE DEVICE, PRESENT MOBILE VERSION.

TARGET 250 COMPLETES FOR EACH OF THE GROUPS]

	Number of Completes	Stimuli Description
GROUP A (Splash Screen Only)	250	<ul style="list-style-type: none"> <li>• Incognito Splash Screen</li> <li>• “Learn More” page</li> </ul>
GROUP B (Splash Screen with Policies (Highlighted))	250	<ul style="list-style-type: none"> <li>• Google Privacy Policy, March 31, 2020 (with and without highlights)</li> <li>• Chrome Privacy Notice, May 20, 2020 (with and without highlights)</li> <li>• Incognito Splash Screen</li> <li>• “Learn More” page</li> </ul>
GROUP C (Splash Screen with New Account Creation Agreement)	250	<ul style="list-style-type: none"> <li>• New Account Creation Agreement</li> <li>• Incognito Splash Screen</li> <li>• “Learn More” page</li> </ul>
GROUP D (Splash Screen with Consent Bump Agreement and FAQ Page)	250	<ul style="list-style-type: none"> <li>• Consent Bump Agreement and FAQ page</li> <li>• Incognito Splash Screen</li> <li>• “Learn More” page</li> </ul>

Q0. Based on your answers to the previous questions, you have qualified for this survey.

[NEXT PAGE]

Q1. This survey is about private browsing mode. You have been selected to answer questions about Chrome, which is a browser from a company named Google.

Next, you will see images of [STIMULI]. Please consider these images with the intention to use private browsing mode. After, you will be asked to answer a few questions. You will be able to view these images again as you answer the questions.

Please do not use your browser's "Back" button.

If you don't know an answer to a question or if you don't have an opinion, please don't guess. Simply indicate this in your response by selecting the "Don't know / Unsure" option or the "I don't feel I have enough information to answer this question" option. There are no right or wrong answers.

[PIPE INTO "STIMULI"]

- "a screen that appears when you enable Chrome's Incognito mode and a page that includes additional information for private browsing" **IF RESPONDENT IS ASSIGNED TO GROUP A,**
- **OR** "[a screen that appears when you enable Chrome's Incognito mode and a page that includes additional information for private browsing], as well as [Google's Privacy Policy] and [the Chrome Privacy Notice]" **IF RESPONDENT IS ASSIGNED TO GROUP B,**
- **OR** "[a screen that appears when you enable Chrome's Incognito mode and a page that includes additional information for private browsing], as well as [Google's terms of service related to saving your web and app activity]" **IF RESPONDENT IS ASSIGNED TO GROUPS C OR D.**

**ORDER BRACKETED TEXT FOR GROUPS B, C, OR D BASED ON THE ORDER THAT IMAGES ARE PRESENTED TO RESPONDENTS, WHERE Q8/Q9 CORRESPONDS TO "a screen that appears when you enable Chrome's Incognito mode and a page that includes additional information for private browsing" Q2/Q3 CORRESPONDS TO "Google's Privacy Policy", Q4/Q5 CORRESPONDS TO "the Chrome Privacy Notice", AND Q6 OR Q7 CORRESPONDS TO "Google's terms of service related to saving your web and app activity"]**

[NEXT PAGE]

**[IF RESPONDENT IS ASSIGNED TO GROUP A, SHOW BLOCK D (Q8-Q9)]**

**[IF RESPONDENT IS ASSIGNED TO GROUP B, SHOW BLOCK A (Q2-Q5) AND BLOCK D (Q8-Q9)]**

**[IF RESPONDENT IS ASSIGNED TO GROUP C, SHOW BLOCK B (Q6) AND BLOCK D (Q8-Q9)]**

**[IF RESPONDENT IS ASSIGNED TO GROUP D, SHOW BLOCK C (Q7) AND BLOCK D (Q8-Q9)]**

[RANDOMIZE ORDER OF BLOCKS PRESENTED. WITHIN BLOCK A, RANDOMIZE ORDER OF BLOCK A.1 (Q2-Q3) AND A.2 (Q4-Q5)]

[BLOCK A]

[BLOCK A.1]

Q2. You will now see the Google Privacy Policy. Please carefully read this policy. Within the policy, hyperlinks have been disabled; however, if you click on [TOC], you will be able to navigate to specific policy sections. **Please scroll through the window below to see the whole image. The continue button can be found at the bottom of the page.**

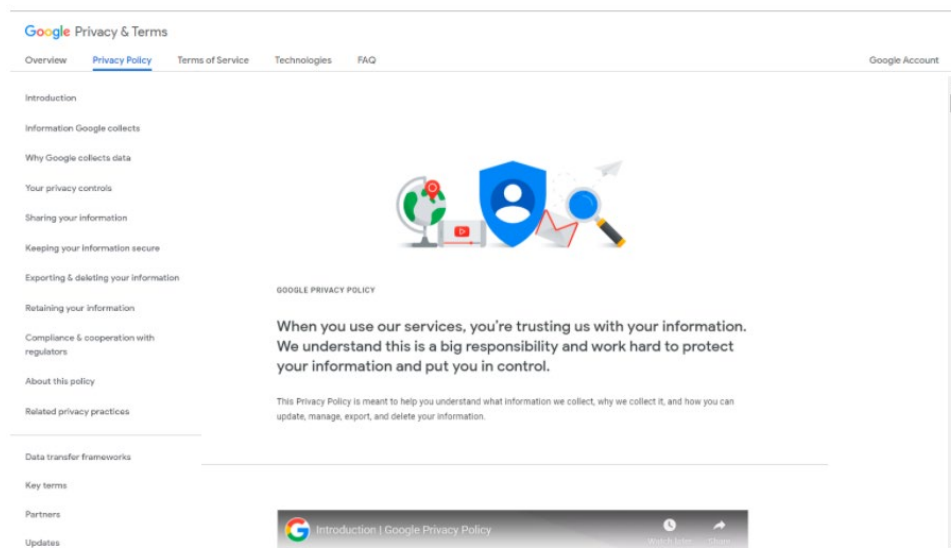
Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

[PIPE INTO “TOC” “certain Table of Contents section headings on the left-hand side” IF RESPONDENT IS USING DESKTOP DEVICE OR “the Table of Contents section headings near the top of the page” IF RESPONDENT IS USING MOBILE DEVICE]

[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]

[DISPLAY PRIVACY POLICY IMAGE]

[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 30 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 30. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]



[NEXT PAGE]

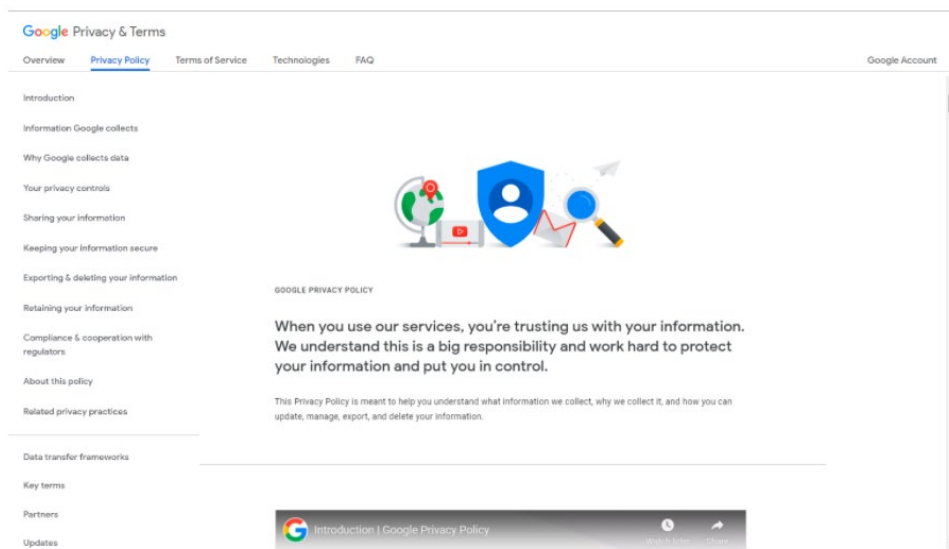
- Q3. Thank you for reviewing the [Google Privacy Policy](#). Before continuing, please take another look at the highlighted sections and make sure you understand them. As you answer questions, you will be able to review the policy again. **Please scroll through the window below to see the whole image. The continue button can be found at the bottom of the page.**

Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

**[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]**

**[DISPLAY HIGHLIGHTED VERSION OF PRIVACY POLICY IMAGE]**

**[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 15 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 15. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]**



**[NEXT PAGE]**

[BLOCK A.2]

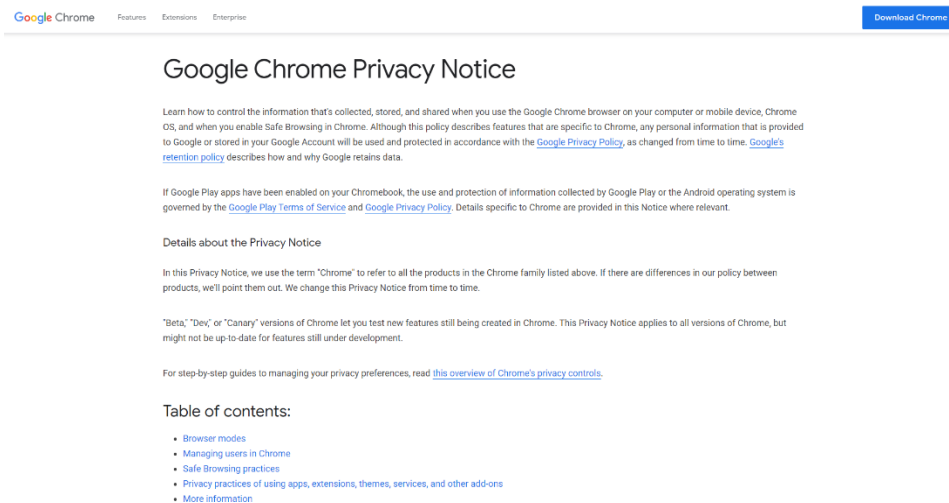
Q4. You will now see the Chrome Privacy Notice. Please read it carefully. Within the policy, hyperlinks have been disabled; however, you can navigate to specific sections of the policy by clicking on the headings under the Table of Contents. **Please scroll through the window below to see the whole image. The continue button can be found at the bottom of the page.**

Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]

[DISPLAY CHROME PRIVACY NOTICE IMAGE]

[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 30 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 30. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]



[NEXT PAGE]

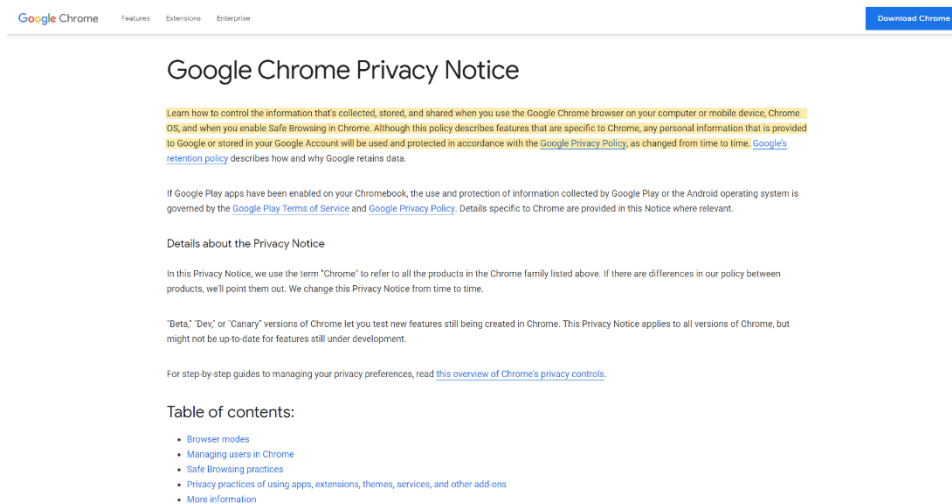
Q5. Thank you for reviewing the [Chrome Privacy Notice](#). Before continuing, please take another look at the highlighted sections and make sure you understand them. As you answer questions, you will be able to review the notice again. **Please scroll through the window below to see the whole image. The continue button can be found at the bottom of the page.**

Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

**[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]**

**[DISPLAY HIGHLIGHTED VERSION OF CHROME PRIVACY NOTICE]**

**[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 15 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 15. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]**



**[NEXT PAGE]**

[BLOCK B]

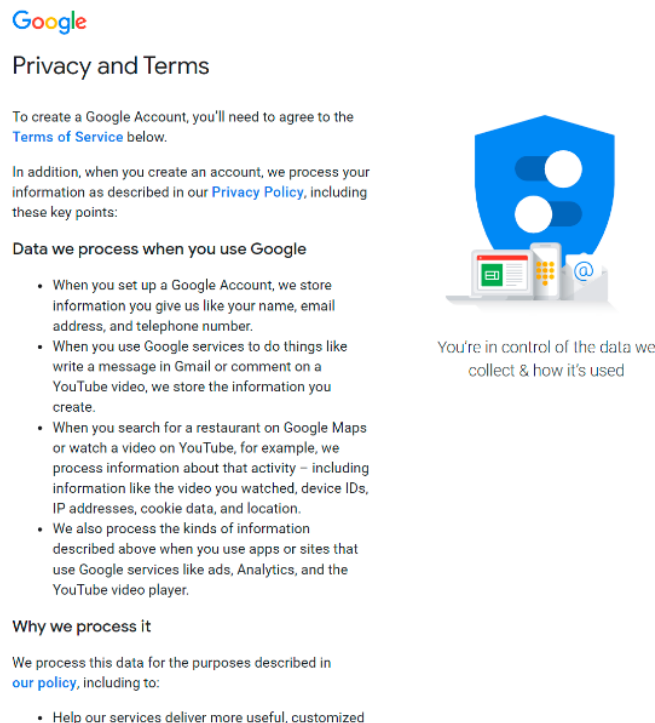
Q6. You will now see the terms of service related to saving your web and app activity. Please carefully read this agreement. Within the agreement, hyperlinks have been disabled. **Please scroll through the window below to see the whole image. The continue button can be found at the bottom of the page.**

Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]

[DISPLAY NEW ACCOUNT CREATION AGREEMENT IMAGE]

[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 30 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 30. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]



[NEXT PAGE]



[BLOCK C]

- Q7. You will now see the terms of service related to saving your web and app activity. Please carefully read this agreement. Within the agreement, hyperlinks have been disabled. **Please scroll through the window below to see the whole image. The continue button can be found at the bottom of the page.**

Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]

[DISPLAY CONSENT BUMP AGREEMENT AND FAQ PAGE IMAGE]

[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 30 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 30. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]



### Some new features for your Google Account

We've introduced some optional features for your account, giving you more control over the data Google collects and how it's used, while allowing Google to show you more relevant ads.

What changes if you turn on these new features?

1. More information will be available in your *Google Account*, making it easier for you to review and control



When you use Google services like Search and YouTube, you generate data – things like what you've searched for and videos you've watched. You can find and control that data in *My Account* under the **Web & App Activity** setting.

With this change, this setting may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.

2. Google will use this information to make ads across the web more relevant for you



[NEXT PAGE]

**[BLOCK D]**

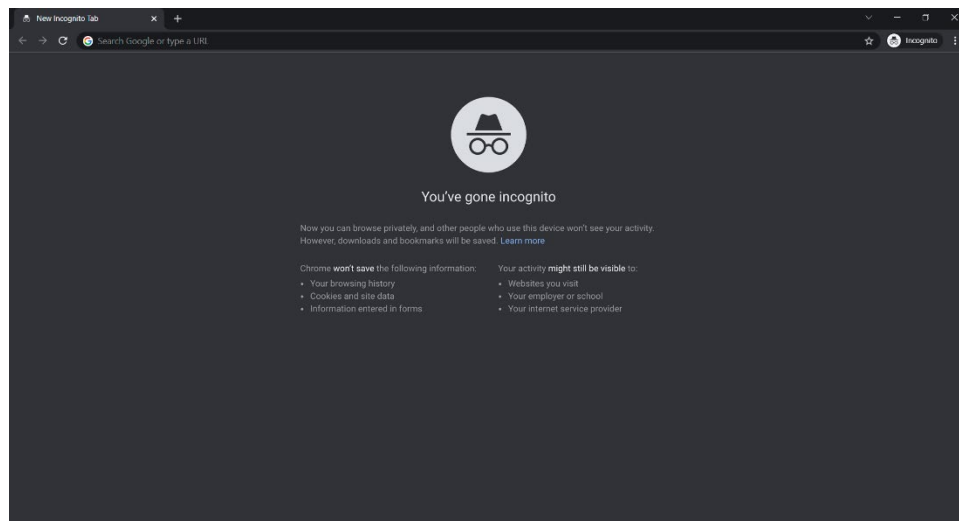
Q8. You will now see the screen that appears when a new Chrome Incognito window is opened. Please read the page carefully. Hyperlinks have been enabled in this image.

Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

**[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]**

**[DISPLAY INCOGNITO SPLASH SCREEN IMAGE]**

**[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 30 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 30. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]**



**[CREATE HYPERLINK TO “LEARN MORE” ON THE IMAGE AND RECORD WHETHER OR NOT RESPONDENT CLICKS ON IT.]**

- **IF RESPONDENT CLICKS ON “LEARN MORE” BEFORE THE 30-SECOND TIMER EXPIRES, PRESENT A POP UP WITH THE FOLLOWING MESSAGE, “YOU WILL BE TAKEN TO THE NEXT PAGE IN [X] SECONDS.” WHERE X IS A TIMER THAT MIRRORS THE NUMBER OF SECONDS REMAINING IN THE 30-SECOND TIMER FOR THE PAGE. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP. TAKE RESPONDENT TO Q9 WHEN THE TIMER EXPIRES.**
- **IF RESPONDENT CLICKS ON “LEARN MORE” AFTER THE 30-SECOND TIMER EXPIRES, TAKE RESPONDENT TO Q9.**

**CLICKING THE “CONTINUE” BUTTON AFTER THE TIMER EXPIRES WILL ALSO TAKE RESPONDENT TO Q9]**

**[NEXT PAGE]**

Q9. You will now see the following screen that would appear if you clicked “Learn more” on the previous page. Hyperlinks and any other clickable elements in this image have been disabled.

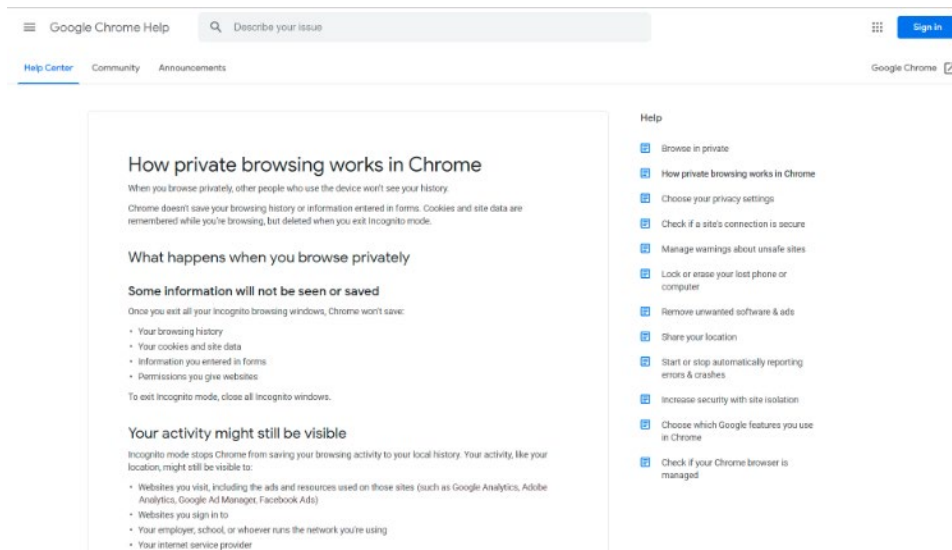
Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

**[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]**

**[DISPLAY “LEARN MORE” PAGE IMAGE]**

**[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 30 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 30. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]**

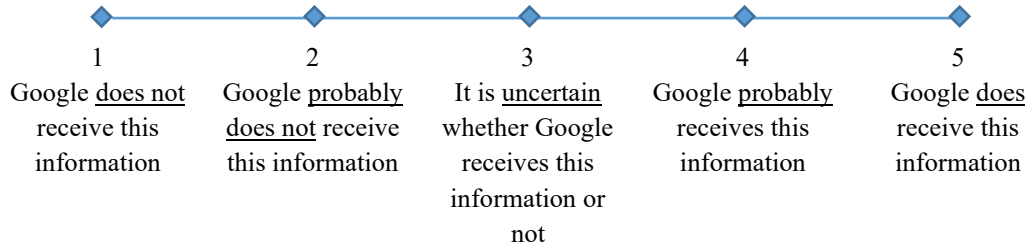
**[PROGRAM THE “LEARN MORE” PAGE IMAGE TO BE SCROLLABLE WITHIN THE BROWSER WINDOW FRAME]**



**[NEXT PAGE]**



- Q11. Based on the screens that you reviewed, please select one of the following regarding IP address during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product):  
(Select a point on the scale. If you do not have enough information, please select “I don’t feel I have enough information to answer this question”)

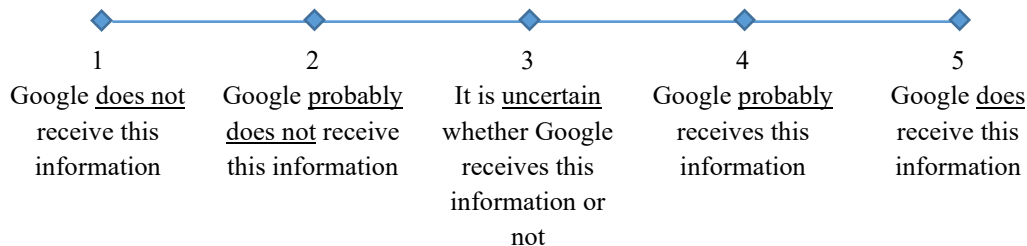


Ⓐ I don’t feel I have enough information to answer this question [EXCLUSIVE]

[IF RESPONDENT HOVERS OVER “IP ADDRESS” IN THE QUESTION, DISPLAY THE FOLLOWING TEXT, “Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. An IP address can often be used to identify the location from which a device is connecting to the Internet.”]

[NEXT PAGE]

- Q12. Based on the screens that you reviewed, please select one of the following regarding cookies placed on your browser during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product):  
(Select a point on the scale. If you do not have enough information, please select “I don’t feel I have enough information to answer this question”)



Ⓐ I don’t feel I have enough information to answer this question [EXCLUSIVE]

[IF RESPONDENT HOVERS OVER “COOKIES” IN THE QUESTION, DISPLAY THE FOLLOWING TEXT, “A small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information.”]

[NEXT PAGE]

### Follow Up Questions

QF1. Were you or were you not able to view the images clearly to answer the questions asked in this survey? *(Select only one option)*

**[RANDOMIZE ORDER; KEEP “DON’T KNOW / UNSURE” LAST]**

- ☐ I was able to view the images clearly to answer the questions asked in this survey
- ☐ I was not able to view the images clearly to answer the questions asked in this survey
- ☐ Don’t know / Unsure **[ANCHOR LAST]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QF2. Prior to this survey, were you or were you not aware of any lawsuits related to private browsing mode? *(Select only one option)*

**[USE THE SAME ORDER OF HAVE/HAVE NOT ANSWERS AS IN QF1]**

- ☐ I was aware of at least one lawsuit related to private browsing mode
- ☐ I was not aware of any lawsuit related to private browsing mode **[SKIP TO QF4]**
- ☐ Don’t know / Unsure **[ANCHOR LAST; SKIP TO QF4]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QF3. You indicated that you were aware of at least one lawsuit regarding private browsing mode. Please describe the lawsuit(s) you were aware of: *(Please type in your response. If you do not know the answer or are unsure, please select “Don’t know / Unsure”)*

**[OPEN-ENDED TEXT BOX, LIMITING TO 1000 CHARACTERS]**

**[REQUIRE AT LEAST 4 CHARACTERS; SHOW ERROR “Please be thorough in your response.”**

**IF ENTRY IS LESS THAN 4 CHARACTERS]**

- ☐ Don’t know / Unsure **[EXCLUSIVE]**

**[IF NO RESPONSE IS PROVIDED, DISPLAY TEXT “PLEASE TYPE A RESPONSE OR SELECT DON’T KNOW / UNSURE.”]**

**[NEXT PAGE]**

QF4. In the past three months, have you or have you not taken any other survey related to private browsing mode? (*Select only one option*)

**[USE THE SAME ORDER OF HAVE/HAVE NOT ANSWERS AS IN QF1]**

- ☐ I have taken a survey related to private browsing mode
- ☐ I have not taken a survey related to private browsing mode
- ☐ Don't know / Unsure **[ANCHOR LAST]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT "PLEASE SELECT AN ANSWER."]**

**[GO TO PANEL THANK YOU PAGE]**



# **APPENDIX F.3**

## **LIKELIHOOD OF USE SURVEY INSTRUMENT**

**Likelihood of Use Experimental Survey Instrument  
Survey Programmer Instructions**

**LEGEND:**

**[PROGRAMMER NOTES IN BOLD CAPS AND BRACKETS]**

*Notes to respondent in italics*

**FORMAT:** The survey consists of the following sections:

<b>Introduction &amp; Screening</b> (questions labeled QS)
<b>Main Survey Questions</b> (questions labeled Q)
<b>Follow-Up Questions</b> (questions labeled QF)

**Overview**

**[NATIONAL 18+ SAMPLE]**

**[PANEL MEMBERS SHOULD BE MATCHED TO THE CENSUS ON AGE, GENDER, AND REGION. THAT IS, THE SCREENER SHOULD BE APPLIED TO A SAMPLE REPRESENTATIVE OF THE GENERAL POPULATION IN THE UNITED STATES SO THAT THE FINAL SAMPLE IS REPRESENTATIVE OF THE TARGET POPULATION FOR THE SURVEY (BASED ON ACTUAL QUALIFICATION).]**

**[TARGET 1000 COMPLETES]**

**[DISABLE THE BROWSER'S "BACK" BUTTON AND DO NOT SHOW A "BACK" BUTTON WITHIN THE SURVEY]**

**[FORCE RESPONSES TO ALL QUESTIONS]**

**[NO SURVEY TITLE AND NO QUESTION NUMBER TO BE DISPLAYED TO RESPONDENTS]**

**[DIGITAL FINGERPRINTING SHOULD BE USED TO AVOID REPEAT PARTICIPATION. DO NOT INVITE RESPONDENTS WHO WERE INVITED TO TAKE OTHER SURVEYS IN THIS MATTER]**

**[TEXT FOR TERMINATES: "THANK YOU FOR YOUR INTEREST IN OUR STUDY. WE ARE NO LONGER LOOKING FOR PEOPLE WHO MATCH YOUR CHARACTERISTICS. WE APPRECIATE YOUR TIME."]**

**Introduction and Screening**

QS0. Please enter the code exactly as it appears in the image below and then click "Continue" to continue.

**[INSERT CAPTCHA; TERMINATE IF NOT CORRECT AFTER FOUR TRIES]**

**[IF NO RESPONSE IS SELECTED OR CAPTCHA CODE IS INCORRECT, DISPLAY TEXT  
“PLEASE ENTER THE CORRECT CODE.”]**

**[NEXT PAGE]**

QS1. Thank you for participating in our study. Your opinions are very important to us. If you don't know an answer to a question or if you don't have an opinion, please don't guess. Simply indicate this in your response by selecting the “Don't know / Unsure” option or the “I don't feel I have enough information to answer this question” option. There are no right or wrong answers.

Your answers will be kept in strict confidence and the results of this study will not be used to try to sell you anything. Trademarks and logos are all the intellectual property of their respective owners.

If you wear glasses or corrective lenses when using a desktop computer, laptop computer, mobile phone, or tablet, please wear them throughout the survey.

Please do not use the “Back” button of your browser while taking the survey. This survey will take less than 15 minutes of your time. When you are ready to get started, please select the “Continue” button.

**[NEXT PAGE]**

QS2. What is your age? *(Select only one option)*

**[ROTATE ORDER, AS IS AND REVERSE; KEEP “PREFER NOT TO ANSWER” LAST]**

- ☐ Under 18 **[TERMINATE]**
- ☐ 18 - 29
- ☐ 30 - 39
- ☐ 40 - 49
- ☐ 50 - 59
- ☐ 60 or older
- ☐ Prefer not to answer **[ANCHOR LAST; TERMINATE]**

**[TERMINATE IF AGE DOES NOT MATCH THE VALUE PASSED BY PANEL PROVIDER]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QS3. Are you...? *(Select only one option)*

**[ROTATE ORDER, AS IS AND REVERSE; KEEP “OTHER” AND “PREFER NOT TO ANSWER” LAST]**

- ☐ Male
- ☐ Female
- ☐ Other **[ANCHOR SECOND TO LAST]**
- ☐ Prefer not to answer **[ANCHOR LAST; TERMINATE]**

**[TERMINATE IF GENDER DOES NOT MATCH THE VALUES PASSED BY PANEL PROVIDER ONLY IF “MALE” OR “FEMALE” IS SELECTED]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QS4. In which state do you live? *(Select only one option)*

**[DROP DOWN MENU OF 50 STATES + DISTRICT OF COLUMBIA; HIDDEN VARIABLE FOR REGION; DETERMINE US CENSUS REGION BASED ON STATE SELECTED. ADD “PREFER NOT TO ANSWER” AND “DON’T KNOW / UNSURE” OPTIONS BELOW DROP DOWN MENU]**

- ☐ Prefer not to answer **[ANCHOR SECOND TO LAST; TERMINATE]**
- ☐ Don’t know / Unsure **[ANCHOR LAST; TERMINATE]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT EITHER A STATE, PREFER NOT TO ANSWER, OR DON’T KNOW / UNSURE.”]**

**[NEXT PAGE]**

QS5. Have you or any member of your household ever worked for any of the following types of companies? *(Select all that apply)*

**[RANDOMIZE LIST; KEEP “NONE OF THE ABOVE” LAST]**

- ☐ A technology company or technology consultancy
- ☐ A law firm, legal services organization, or court **[TERMINATE]**
- ☐ A marketing, market research, or advertising agency
- ☐ An academic institution
- ☐ A construction company
- ☐ A clothing retailer
- ☐ A real estate agency
- ☐ A car dealership
- ☐ A fitness center
- ☐ A healthcare provider or medical office
- ☐ None of the above **[ANCHOR LAST; EXCLUSIVE]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT THE RELEVANT COMPANY TYPE(S) OR NONE OF THE ABOVE.”]**

**[NEXT PAGE]**

QS6. This question is to check your attention. Please select “South” from the answer options below.  
(*Select only one option*)

**[RANDOMIZE ORDER; KEEP “NONE OF THE ABOVE” AND “DON’T KNOW / UNSURE” LAST]**

- ☐ North
- ☐ East
- ☐ South
- ☐ West
- ☐ None of the above **[ANCHOR SECOND TO LAST]**
- ☐ Don’t know / Unsure **[ANCHOR LAST]**

**[TERMINATE IF “SOUTH” IS NOT SELECTED]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QS7. Thinking about the device(s) you use to browse the internet (such as your phone, your personal laptop, or your office computer), which internet browser(s) do you currently use? (*Select all that apply*)

**[RANDOMIZE LIST; KEEP “OTHER” AND “DON’T KNOW / UNSURE” LAST]**

- ☐ Internet Explorer
- ☐ Microsoft Edge
- ☐ Safari
- ☐ Brave
- ☐ Google Chrome
- ☐ Mozilla Firefox
- ☐ Opera
- ☐ DuckDuckGo
- ☐ Odeon **[TERMINATE]**
- ☐ Other (*Please specify*) \_\_\_\_\_ **[ANCHOR SECOND TO LAST]**
- ☐ Don’t know / Unsure **[ANCHOR LAST; EXCLUSIVE]**

**[TERMINATE IF ANY COMBINATION OF ANSWER OPTIONS CONTAINING “ODEON” IS SELECTED]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT EITHER THE INTERNET BROWSER(S) YOU USE OR DON’T KNOW / UNSURE.”]**

**[NEXT PAGE]**

QS8. In the past six months, which of the following features, if any, have you used on your internet browser(s)? (*Select all that apply*)

[RANDOMIZE LIST; KEEP “OTHER” AND “DON’T KNOW / UNSURE” LAST]

- ☐ Private browsing mode
- ☐ Bookmarks
- ☐ Website translator
- ☐ Customized home page
- ☐ Screenshot tool
- ☐ Dark mode for visual display
- ☐ Other (*Please specify*) \_\_\_\_\_ [ANCHOR SECOND TO LAST]
- ☒ Don’t know / Unsure [ANCHOR LAST; EXCLUSIVE]

[TERMINATE IF “PRIVATE BROWSING MODE” IS NOT SELECTED]

[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT THE FEATURES YOU USED ON YOUR INTERNET BROWSER(S) OR SELECT DON’T KNOW / UNSURE.”]

[NEXT PAGE]

## Main Questionnaire

[ASSIGN RESPONDENT TO CELLS BASED ON THE FOLLOWING:

FIRST, ASSIGN RESPONDENT TO LANGUAGE GROUP:

- RANDOMIZE RESPONDENT TO “ACTUAL LANGUAGE” OR “ALTERNATIVE LANGUAGE” GROUP.

SECOND, ASSIGN RESPONDENT TO MOBILE OR DESKTOP VERSION:

- DETECT DEVICE RESPONDENT IS USING.
- IF RESPONDENT IS USING A DESKTOP COMPUTER, LAPTOP COMPUTER, OR TABLET, PRESENT DESKTOP VERSION.
- IF RESPONDENT IS USING A MOBILE DEVICE, PRESENT MOBILE VERSION.

TARGET 500 COMPLETES FOR EACH OF THE “ACTUAL LANGUAGE” AND “ALTERNATIVE LANGUAGE” GROUPS]

Mobile or Desktop Version	GROUP	
	Actual Language 500 completes	Alternative Language 500 completes
Desktop	Actual language	Alternative language
Mobile		

Q0. Based on your answers to the previous questions, you have qualified for this survey.

[NEXT PAGE]

Q1. You will first be presented with a scenario. Next, you will see an image. After, you will be asked to answer a few questions. You will be able to view any images again as you answer the questions.

Please do not use your browser’s “Back” button.

If you don’t know an answer to a question or if you don’t have an opinion, please don’t guess. Simply indicate this in your response by selecting the “Don’t know / Unsure” option or the “I don’t feel I have enough information to answer this question” option. There are no right or wrong answers.

[NEXT PAGE]

- Q2. Imagine that you are researching online about a sensitive topic. You decide to browse the web in private browsing mode.

On the next page, you will see an image of the Chrome browser in Incognito mode.

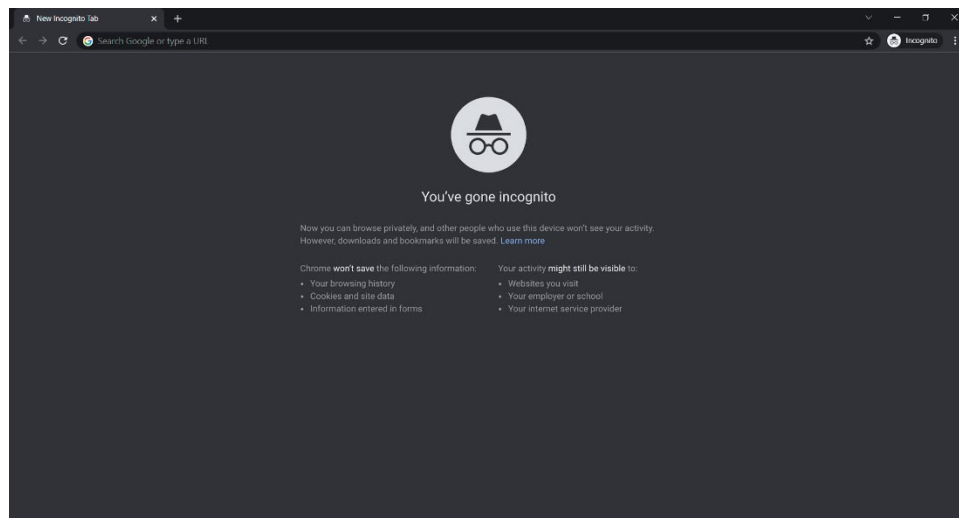
[NEXT PAGE]

- Q3. Please review the page below. Hyperlinks have been enabled in this image.  
Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

**[WHEN USER CLICKS “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]**

**[DISPLAY INCOGNITO SPLASH SCREEN IMAGE]**

**[RESPONDENT MUST VIEW IMAGE FOR AT LEAST 30 SECONDS BEFORE NAVIGATING TO THE NEXT IMAGE. DISPLAY THE INSTRUCTION “(YOU WILL BE ALLOWED TO PROCEED TO THE NEXT SCREEN IN [X] SECONDS.)” WHERE X IS A TIMER COUNTING DOWN FROM 30. WHEN X=0, REMOVE THIS INSTRUCTION AND SHOW THE “CONTINUE” BUTTON]**



**[CREATE HYPERLINK TO “LEARN MORE” ON THE IMAGE AND RECORD WHETHER OR NOT RESPONDENT CLICKS ON IT.]**

- **IF RESPONDENT CLICKS ON “LEARN MORE” BEFORE THE 30-SECOND TIMER EXPIRES, PRESENT A POP UP WITH THE FOLLOWING MESSAGE, “YOU WILL BE TAKEN TO THE NEXT PAGE IN [X] SECONDS.” WHERE X IS A TIMER THAT MIRRORS THE NUMBER OF SECONDS REMAINING IN THE 30-SECOND TIMER FOR THE PAGE. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP. TAKE RESPONDENT TO Q4 WHEN THE TIMER EXPIRES.**



- IF RESPONDENT CLICKS ON “LEARN MORE” AFTER THE 30-SECOND TIMER EXPIRES, TAKE RESPONDENT TO Q4.

IF RESPONDENT DOES NOT CLICK ON HYPERLINK, GO TO Q5 WHEN THEY CLICK ON THE “CONTINUE” BUTTON]

[NEXT PAGE]

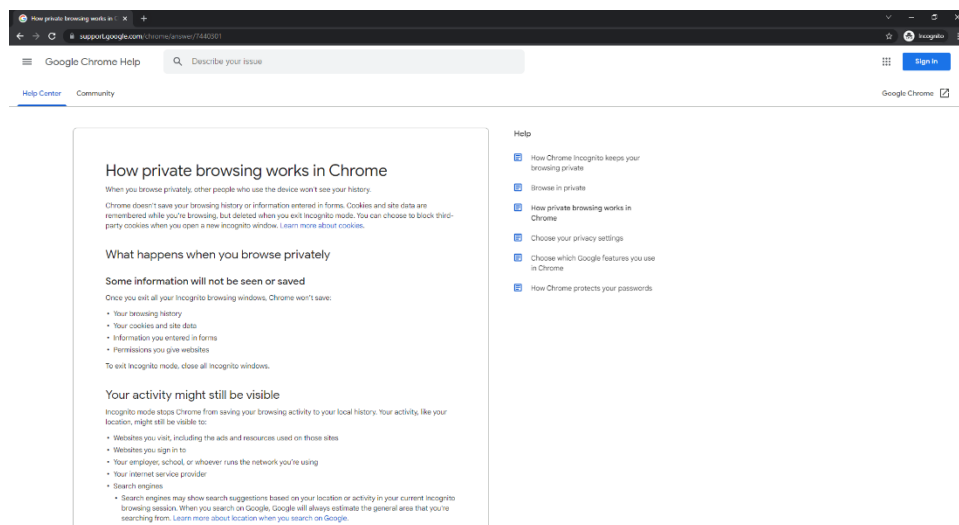
Q4. You see the following screen after clicking “Learn more” on the previous page. Hyperlinks and any other clickable elements in this image have been disabled.

Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.

[WHEN USER CLICKS ON “CLICK HERE TO ZOOM IN ON THE IMAGE. IF YOU CLICK TO ZOOM IN, PLEASE DRAG THE IMAGE TO SCROLL.”, OPEN A POP UP OF THE IMAGE THAT ALLOWS RESPONDENT TO ZOOM IN. ALLOW RESPONDENT THE OPTION TO CLOSE THE POP UP]

[DISPLAY “LEARN MORE” PAGE IMAGE]

[PROGRAM THE “LEARN MORE” PAGE IMAGE TO BE SCROLLABLE WITHIN THE BROWSER WINDOW FRAME]



[NEXT PAGE]

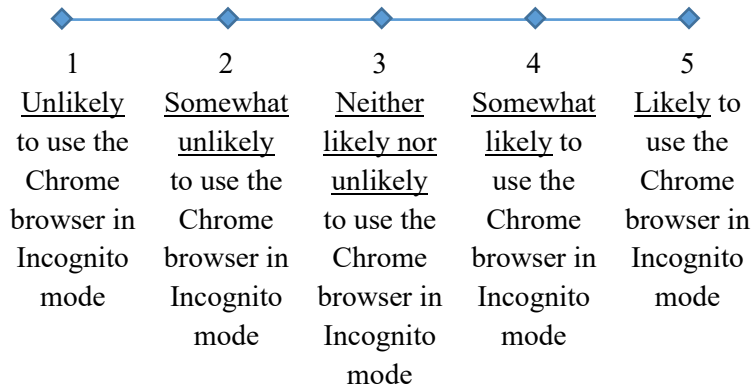
[PRESENT ALL IMAGES THAT THE RESPONDENT REVIEWED AS THUMBNAIL IMAGES AT THE BOTTOM OF THE PAGE FOR Q5]

[AT THE TOP OF EACH PAGE FOR Q5, DISPLAY THE FOLLOWING TEXT IF RESPONDENTS VIEWED ONLY ONE IMAGE: “(The thumbnail contains the image that you have viewed earlier. You can click on the thumbnail to see the enlarged version of this image.)”. DISPLAY

**THE FOLLOWING TEXT IF RESPONDENTS VIEWED MORE THAN ONE IMAGE:** “(The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.)”]

- Q5. How likely or unlikely are you to use the Chrome browser in Incognito mode for your online research about the sensitive topic mentioned in the previous scenario?  
*(Select a point on the scale. If you do not have enough information, please select “I don’t feel I have enough information to answer this question.”)*

**[RANDOMIZE ORDER OF FIRST 5 OPTIONS BETWEEN 1-2-3-4-5 OR 5-4-3-2-1, NO STARTING POINT. DO NOT SHOW NUMBERS ON SCALE TO RESPONDENTS]**



☉ I don’t feel I have enough information to answer this question **[EXCLUSIVE]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

**Follow Up Questions**

**[IN THE BRACKETS IN QF1, DISPLAY “IMAGE” IF RESPONDENT REVIEWED ONE IMAGE AND “IMAGES” IF RESPONDENT REVIEWED MORE THAN ONE IMAGE]**

QF1. Were you or were you not able to view the [image / images] clearly to answer the questions asked in this survey? *(Select only one option)*

**[RANDOMIZE ORDER; KEEP “DON’T KNOW / UNSURE” LAST]**

- ☐ I was able to view the [image / images] clearly to answer the questions asked in this survey
- ☐ I was not able to view the [image / images] clearly to answer the questions asked in this survey
- ☐ Don’t know / Unsure **[ANCHOR LAST]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QF2. Prior to this survey, were you or were you not aware of any lawsuits related to private browsing mode? *(Select only one option)*

**[USE THE SAME ORDER OF HAVE/HAVE NOT ANSWERS AS IN QF1]**

- ☐ I was aware of at least one lawsuit related to private browsing mode
- ☐ I was not aware of any lawsuit related to private browsing mode **[SKIP TO QF4]**
- ☐ Don’t know / Unsure **[ANCHOR LAST; SKIP TO QF4]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT “PLEASE SELECT AN ANSWER.”]**

**[NEXT PAGE]**

QF3. You indicated that you were aware of at least one lawsuit regarding private browsing mode. Please describe the lawsuit(s) you were aware of: *(Please type in your response. If you do not know the answer or are unsure, please select “Don’t know / Unsure”)*

**[OPEN-ENDED TEXT BOX, LIMITING TO 1000 CHARACTERS]**

**[REQUIRE AT LEAST 4 CHARACTERS; SHOW ERROR “Please be thorough in your response.” IF ENTRY IS LESS THAN 4 CHARACTERS]**

- ☐ Don’t know / Unsure **[EXCLUSIVE]**

**[IF NO RESPONSE IS PROVIDED, DISPLAY TEXT “PLEASE TYPE A RESPONSE OR SELECT DON’T KNOW / UNSURE.”]**

**[NEXT PAGE]**

QF4. In the past three months, have you or have you not taken any other survey related to private browsing mode? (*Select only one option*)

**[USE THE SAME ORDER OF HAVE/HAVE NOT ANSWERS AS IN QF1]**

- ☐ I have taken a survey related to private browsing mode
- ☐ I have not taken a survey related to private browsing mode
- ☐ Don't know / Unsure **[ANCHOR LAST]**

**[IF NO RESPONSE IS SELECTED, DISPLAY TEXT "PLEASE SELECT AN ANSWER."]**

**[GO TO PANEL THANK YOU PAGE]**

**APPENDIX G.1**  
**CONSUMER PERCEPTIONS**  
**AND EXPECTATIONS**  
**SURVEY SCREENSHOTS**  
**(CHROME GROUP)**

0%

Please enter the code exactly as it appears in the image below and then click "Continue" to continue.

XMIJF3

Continue

4%

Thank you for participating in our study. Your opinions are very important to us. If you don't know an answer to a question or if you don't have an opinion, please don't guess. Simply indicate this in your response by selecting the "Don't know / Unsure" option or the "I don't feel I have enough information to answer this question" option. There are no right or wrong answers.

Your answers will be kept in strict confidence and the results of this study will not be used to try to sell you anything. Trademarks and logos are all the intellectual property of their respective owners.

If you wear glasses or corrective lenses when using a desktop computer, laptop computer, mobile phone, or tablet, please wear them throughout the survey.

Please do not use the "Back" button of your browser while taking the survey. This survey will take less than 15 minutes of your time. When you are ready to get started, please select the "Continue" button.

Continue

8%

What is your age?  
(Select only one option)

☐ 60 or older

☐ 50 - 59

☐ 40 - 49

☐ 30 - 39

☐ 18 - 29

☐ Under 18

☐ Prefer not to answer

Continue



12%

Are you...?

*(Select only one option)*

☐ Female

☐ Male

☐ Other

☐ Prefer not to answer

Continue

16%

In which state do you live?

*(Select only one option)*

Select one... ▾

☐ Prefer not to answer

☐ Don't know / Unsure

Continue

25%

Have you or any member of your household ever worked for any of the following types of companies?  
(Select all that apply)

☐ A clothing retailer

☐ A construction company

☐ A marketing, market research, or advertising agency

☐ A law firm, legal services organization, or court

☐ A car dealership

☐ A fitness center

☐ A real estate agency

☐ An academic institution

☐ A healthcare provider or medical office

☐ A technology company or technology consultancy

☐ None of the above

Continue

33%

This question is to check your attention. Please select "South" from the answer options below.  
(Select only one option)

☐ North

☐ East

☐ South

☐ West

☐ None of the above

☐ Don't know / Unsure

Continue

37%

Thinking about the device(s) you use to browse the internet (such as your phone, your personal laptop, or your office computer), which internet browser(s) do you currently use?  
(Select all that apply)

☐ Mozilla Firefox

☐ Opera

☐ Safari

☐ Brave

☐ DuckDuckGo

☐ Microsoft Edge

☐ Internet Explorer

☐ Odeon

☐ Google Chrome

☐ Other (Please specify)

☐ Don't know / Unsure

Continue

46%

In the past six months, which of the following features, if any, have you used on your internet browser(s)?  
(Select all that apply)

☐ Customized home page

☐ Bookmarks

☐ Screenshot tool

☐ Dark mode for visual display

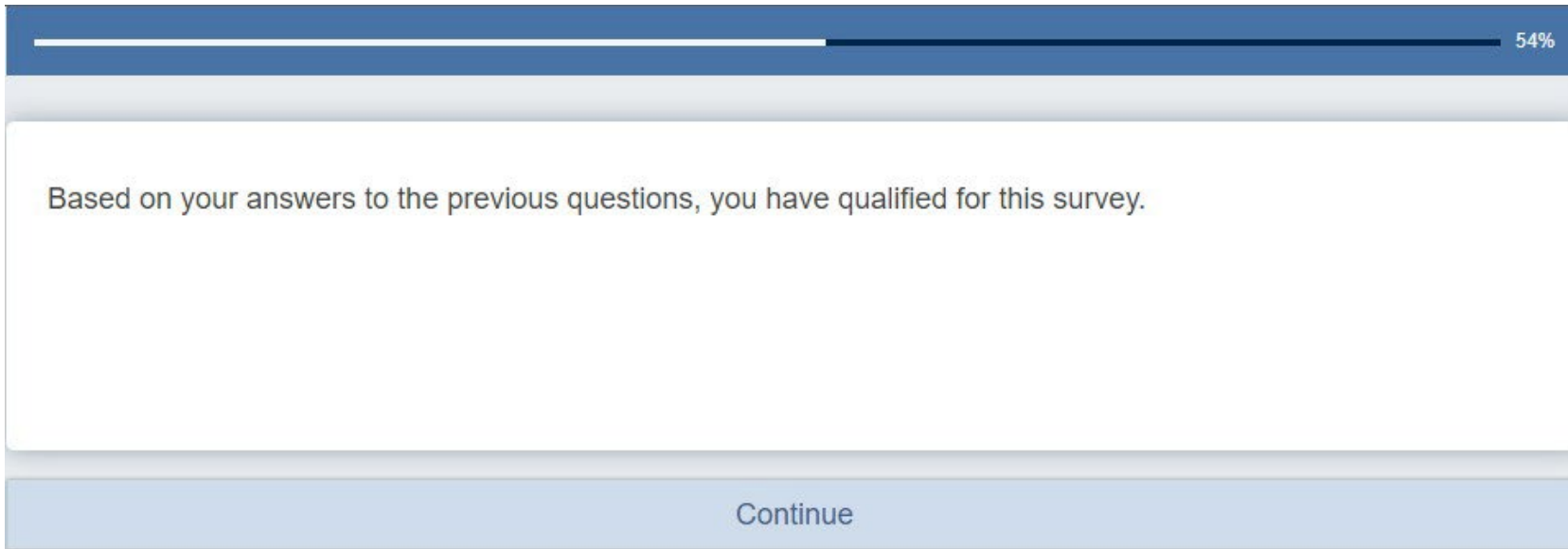
☐ Private browsing mode

☐ Website translator

☐ Other (Please specify)

☐ Don't know / Unsure

Continue



A survey progress bar at the top shows a white line on a blue background, with "54%" indicated on the right. Below the bar is a white box with the text "Based on your answers to the previous questions, you have qualified for this survey." At the bottom is a light blue button labeled "Continue".

54%

Based on your answers to the previous questions, you have qualified for this survey.

Continue

72%

This survey is about what you expect while in private browsing mode. You will first see two images. After, you will be asked to answer a few questions. You will be able to view these images again as you answer the questions.

Please do not use your browser's "Back" button.

If you don't know an answer to a question or if you don't have an opinion, please don't guess. Simply indicate this in your response by selecting the "Don't know / Unsure" option or the "I don't feel I have enough information to answer this question" option. There are no right or wrong answers.

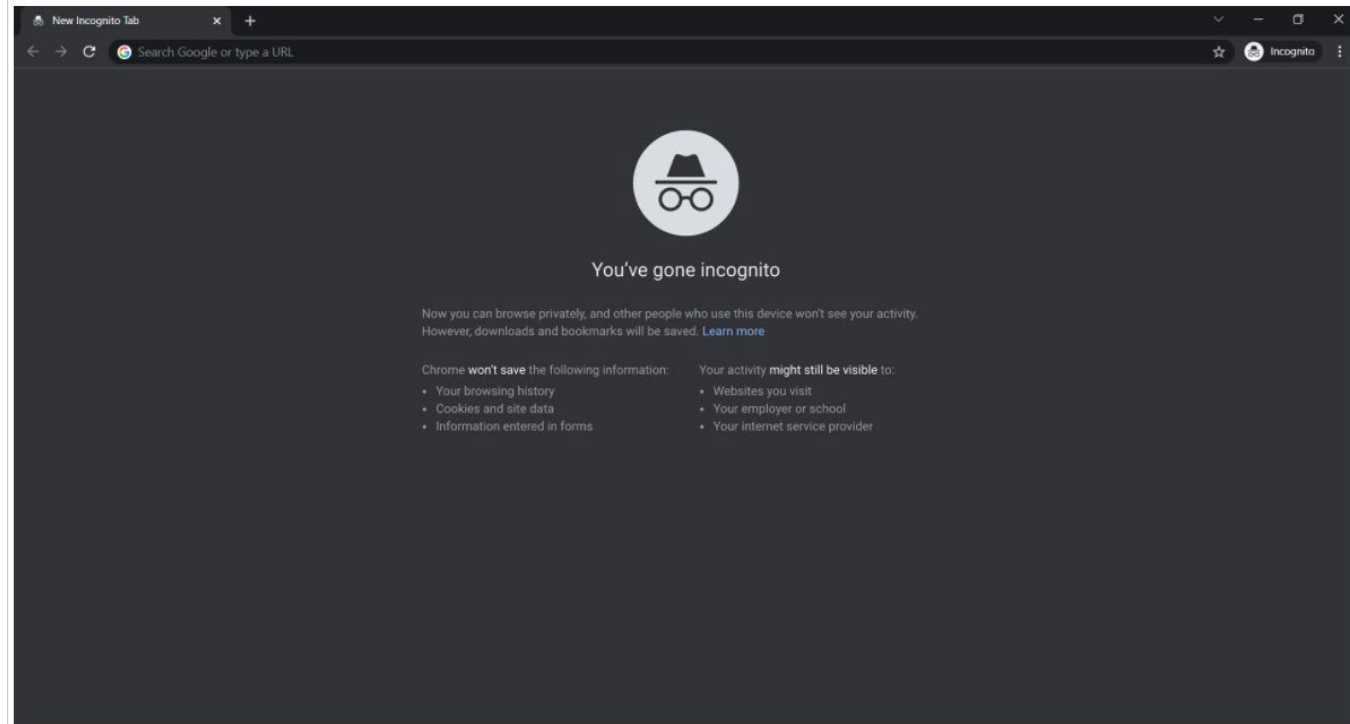
Continue



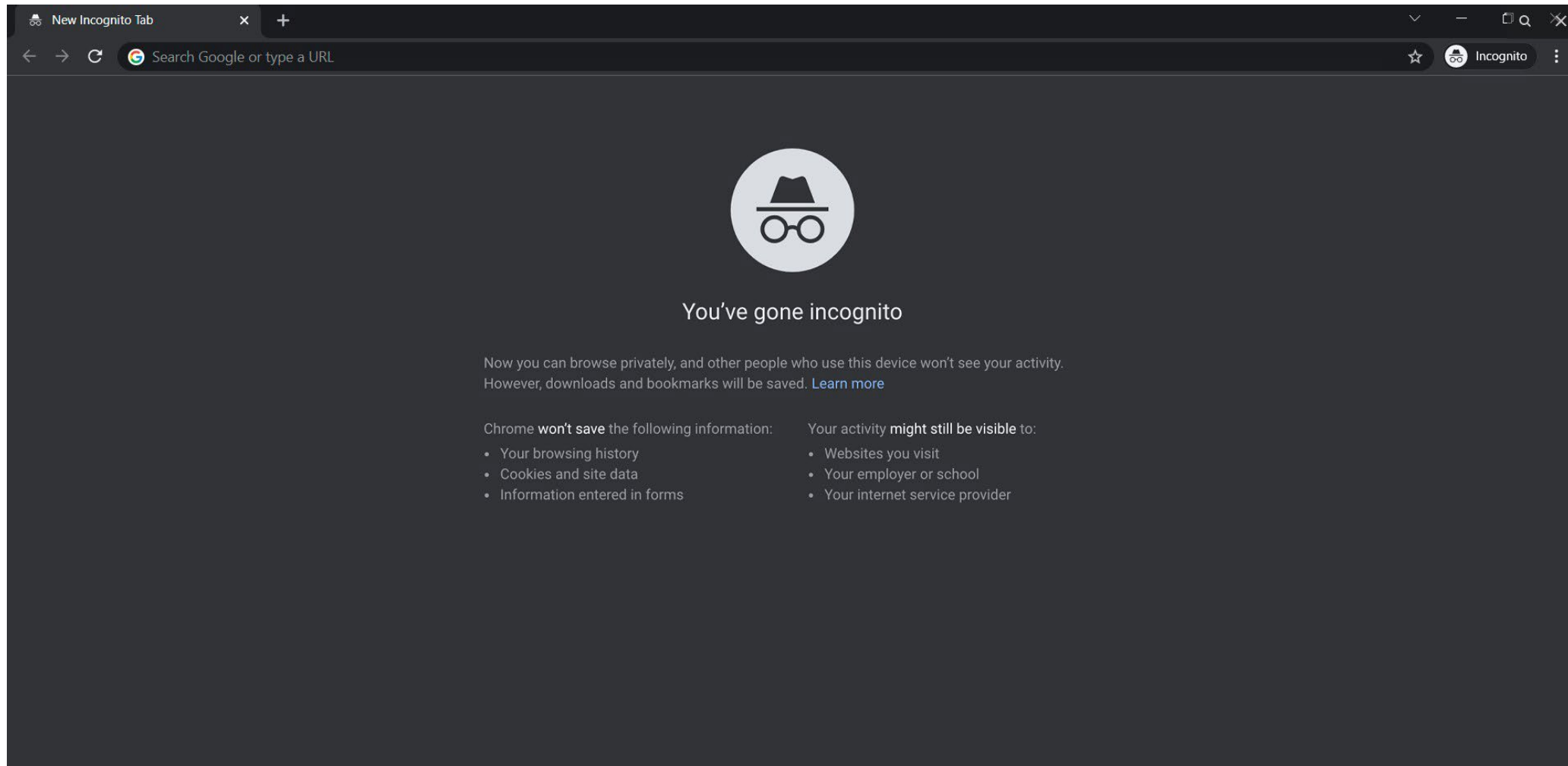
Imagine that you decide to open an Incognito window and see the screen below. Hyperlinks have been enabled in this image.

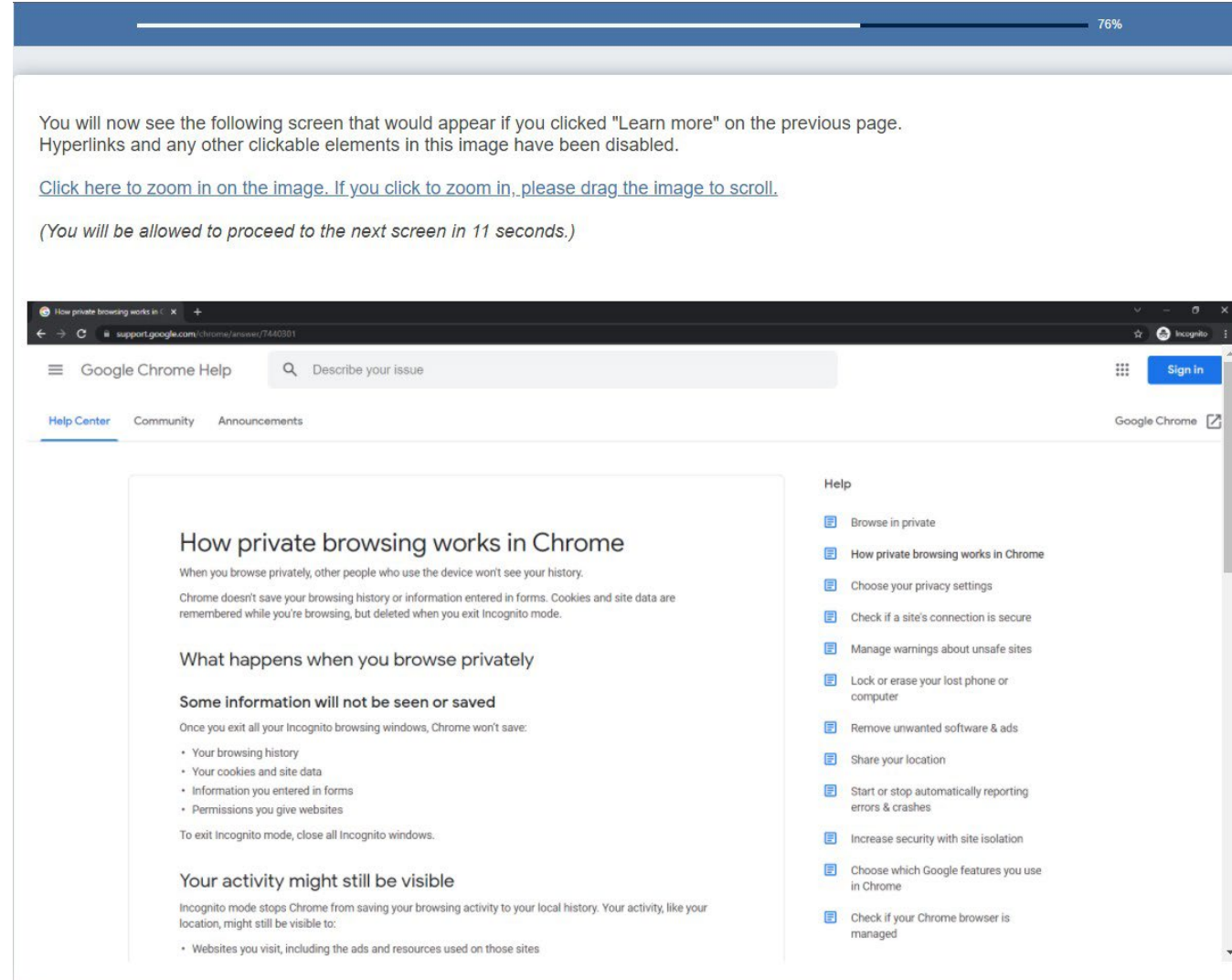
[Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.](#)

*(You will be allowed to proceed to the next screen in 23 seconds.)*

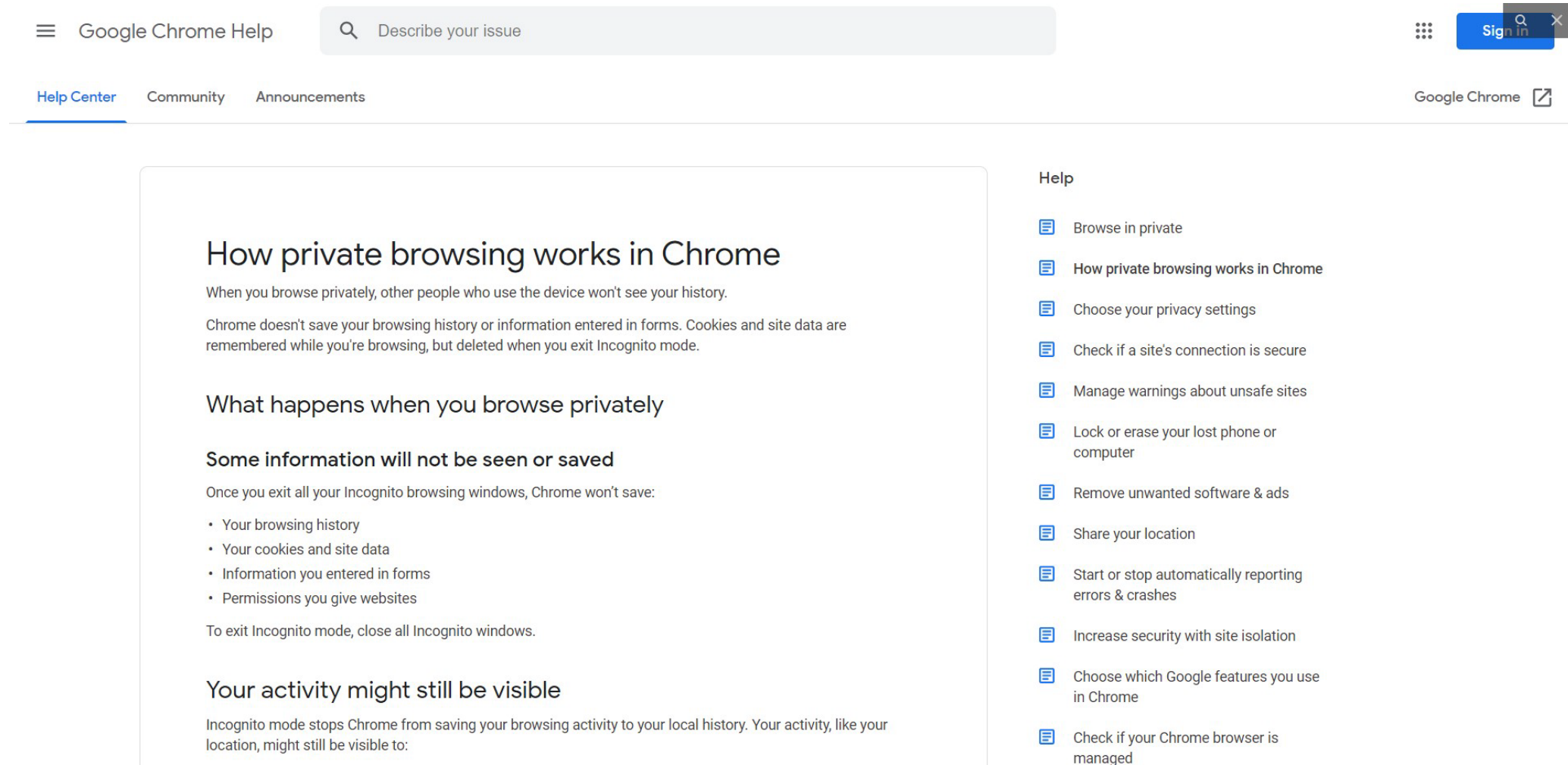


The following is the pop-up window that appears when a respondent clicks to zoom in on the previous page. The respondent can drag to navigate around the image.





The following is the pop-up window that appears when a respondent clicks to zoom in on the previous page. The respondent can drag to navigate around the image.



76%

(The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.)

While in Incognito mode, do the companies that own the websites you visited during the session receive or not receive the data from your Incognito session (such as IP address, URLs of the sites you visit, and cookies)?

Please base your answer on the screens you reviewed.

(Select a point on the scale. If you do not have enough information, please select "I don't feel I have enough information to answer this question")

Companies that own the websites I visited during the session do receive the data from my Incognito session

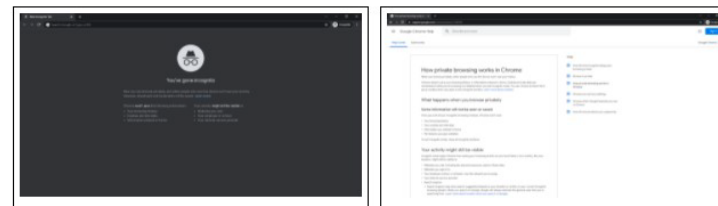
Companies that own the websites I visited during the session probably receive the data from my Incognito session

It is uncertain whether companies that own the websites I visited during the session receive the data from my Incognito session

Companies that own the websites I visited during the session probably do not receive the data from my Incognito session

Companies that own the websites I visited during the session do not receive the data from my Incognito session

☐ I don't feel I have enough information to answer this question



Continue

G.1-16

76%

(The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.)

While in Incognito mode, does your internet service provider receive or not receive the data from your Incognito session (such as **IP address**, **URLs of the sites you visit**, and **cookies**)?

Please base your answer on the screens you reviewed.

(Select a point on the scale. If you do not have enough information, please select "I don't feel I have enough information to answer this question")

My internet service provider does receive the data from my Incognito session


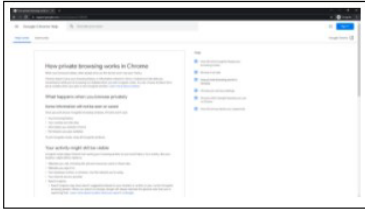
My internet service provider probably receives the data from my Incognito session

It is uncertain whether my internet service provider receives the data from my Incognito session or not

My internet service provider probably does not receive the data from my Incognito session

My internet service provider does not receive the data from my Incognito session

☐ I don't feel I have enough information to answer this question

Continue

76%

(The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.)

While in Incognito mode, do companies that provide analytics and advertising services to websites you visited during the session receive or not receive the data from your Incognito session (such as **IP address**, **URLs of the sites you visit**, and **cookies**)?

Please base your answer on the screens you reviewed.

(Select a point on the scale. If you do not have enough information, please select "I don't feel I have enough information to answer this question")

Companies that provide analytics and advertising services to websites I visited during the session do receive the data from my Incognito session

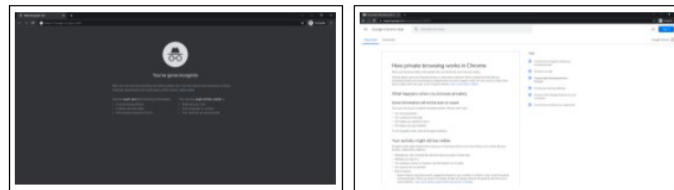
Companies that provide analytics and advertising services to websites I visited during the session probably receive the data from my Incognito session

It is uncertain whether companies that provide analytics and advertising services to websites I visited during the session receive the data from my Incognito session or not

Companies that provide analytics and advertising services to websites I visited during the session probably do not receive the data from my Incognito session

Companies that provide analytics and advertising services to websites I visited during the session do not receive the data from my Incognito session

☐ I don't feel I have enough information to answer this question



Continue

G.1-18

76%

Were you or were you not able to view the images clearly to answer the questions asked in this survey?  
(Select only one option)

☐ I was not able to view the images clearly to answer the questions asked in this survey

☐ I was able to view the images clearly to answer the questions asked in this survey

☐ Don't know / Unsure

Continue



80%

Prior to this survey, were you or were you not aware of any lawsuits related to private browsing mode?  
(Select only one option)

☐ I was not aware of any lawsuit related to private browsing mode

☐ I was aware of at least one lawsuit related to private browsing mode

☐ Don't know / Unsure

Continue

84%

You indicated that you were aware of at least one lawsuit regarding private browsing mode. Please describe the lawsuit(s) you were aware of:

*(Please type in your response. If you do not know the answer or are unsure, please select "Don't know / Unsure")*

☐ Don't know / Unsure

Continue

88%

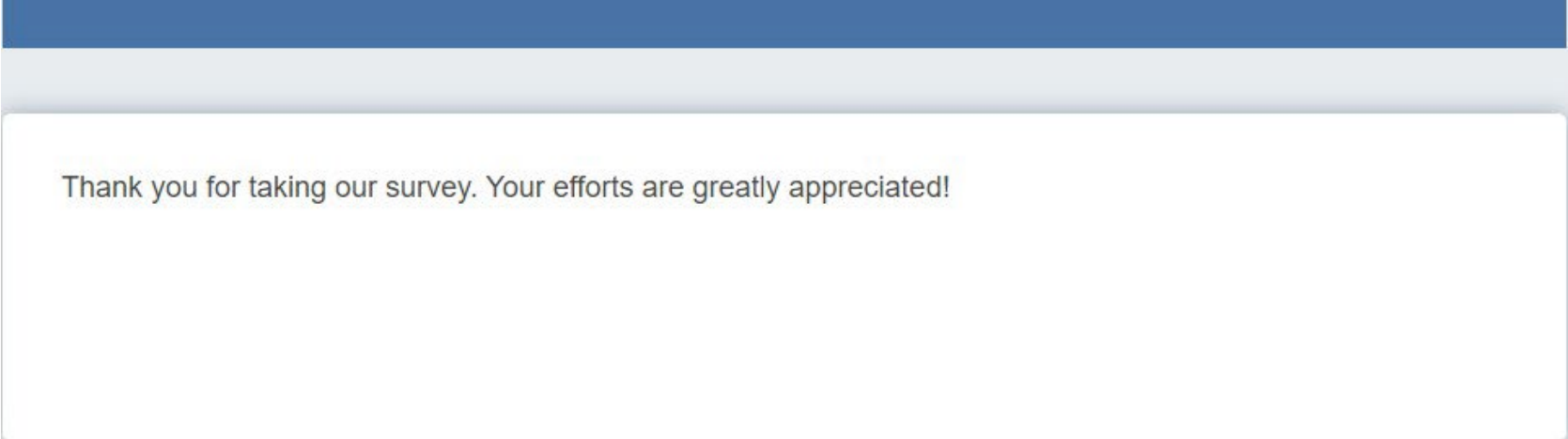
In the past three months, have you or have you not taken any other survey related to private browsing mode?  
(Select only one option)

☐ I have not taken a survey related to private browsing mode

☐ I have taken a survey related to private browsing mode

☐ Don't know / Unsure

Continue



Thank you for taking our survey. Your efforts are greatly appreciated!

**APPENDIX G.2**  
**INTERPRETATION SURVEY**  
**SCREENSHOTS**  
**(SPLASH SCREEN WITH**  
**POLICIES (HIGHLIGHTED)**  
**GROUP)**

0%

Please enter the code exactly as it appears in the image below and then click "Continue" to continue.

8CKHZQ

Continue

2%

Thank you for participating in our study. Your opinions are very important to us. If you don't know an answer to a question or if you don't have an opinion, please don't guess. Simply indicate this in your response by selecting the "Don't know / Unsure" option or the "I don't feel I have enough information to answer this question" option. There are no right or wrong answers.

Your answers will be kept in strict confidence and the results of this study will not be used to try to sell you anything. Trademarks and logos are all the intellectual property of their respective owners.

If you wear glasses or corrective lenses when using a desktop computer, laptop computer, mobile phone, or tablet, please wear them throughout the survey.

Please do not use the "Back" button of your browser while taking the survey. This survey will take less than 15 minutes of your time. When you are ready to get started, please select the "Continue" button.

Continue

5%

What is your age?  
(Select only one option)

☐ 60 or older

☐ 50 – 59

☐ 40 – 49

☐ 30 – 39

☐ 18 – 29

☐ Under 18

☐ Prefer not to answer

Continue



8%

Are you...?

*(Select only one option)*

☐ Female

☐ Male

☐ Other

☐ Prefer not to answer

Continue

11%

In which state do you live?

*(Select only one option)*

Select one... ▼

☐ Prefer not to answer

☐ Don't know / Unsure

Continue

16%

Have you or any member of your household ever worked for any of the following types of companies?  
(Select all that apply)

- ☐ A car dealership
- ☐ A construction company
- ☐ A healthcare provider or medical office
- ☐ A technology company or technology consultancy
- ☐ A clothing retailer
- ☐ An academic institution
- ☐ A marketing, market research, or advertising agency
- ☐ A law firm, legal services organization, or court
- ☐ A fitness center
- ☐ A real estate agency
- ☐ None of the above

Continue

29%

This question is to check your attention. Please select "South" from the answer options below.  
(Select only one option)

☐ East

☐ North

☐ West

☐ South

☐ None of the above

☐ Don't know / Unsure

Continue

32%

Thinking about the device(s) you use to browse the internet (such as your phone, your personal laptop, or your office computer), which internet browser(s) do you currently use?  
(Select all that apply)

☐ Opera

☐ Safari

☐ Odeon

☐ Microsoft Edge

☐ DuckDuckGo

☐ Internet Explorer

☐ Google Chrome

☐ Brave

☐ Mozilla Firefox

☐ Other (Please specify)

☐ Don't know / Unsure

Continue

37%

In the past six months, which of the following features, if any, have you used on your internet browser(s)?  
(Select all that apply)

☐ Screenshot tool

☐ Private browsing mode

☐ Bookmarks

☐ Website translator

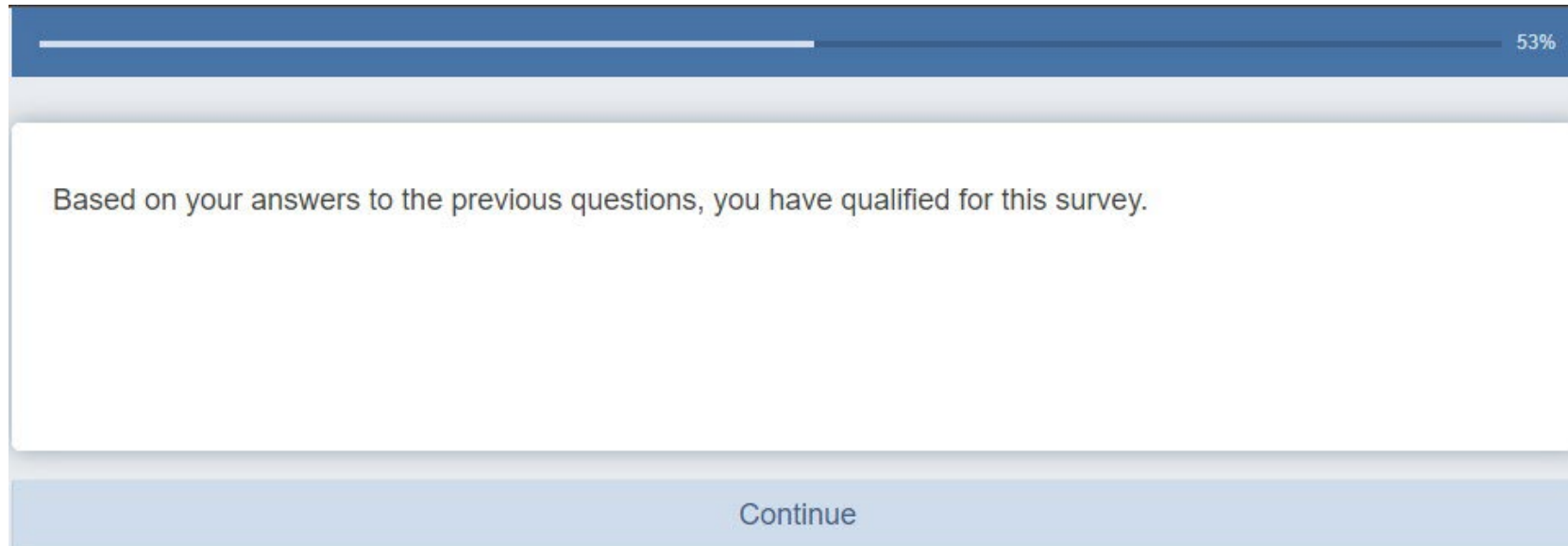
☐ Customized home page

☐ Dark mode for visual display

☐ Other (Please specify)

☐ Don't know / Unsure

Continue



A survey progress bar at the top shows 53% completion. Below it, a white box contains the text: "Based on your answers to the previous questions, you have qualified for this survey." At the bottom is a blue "Continue" button.

53%

Based on your answers to the previous questions, you have qualified for this survey.

Continue

55%

This survey is about private browsing mode. You have been selected to answer questions about Chrome, which is a browser from a company named Google.

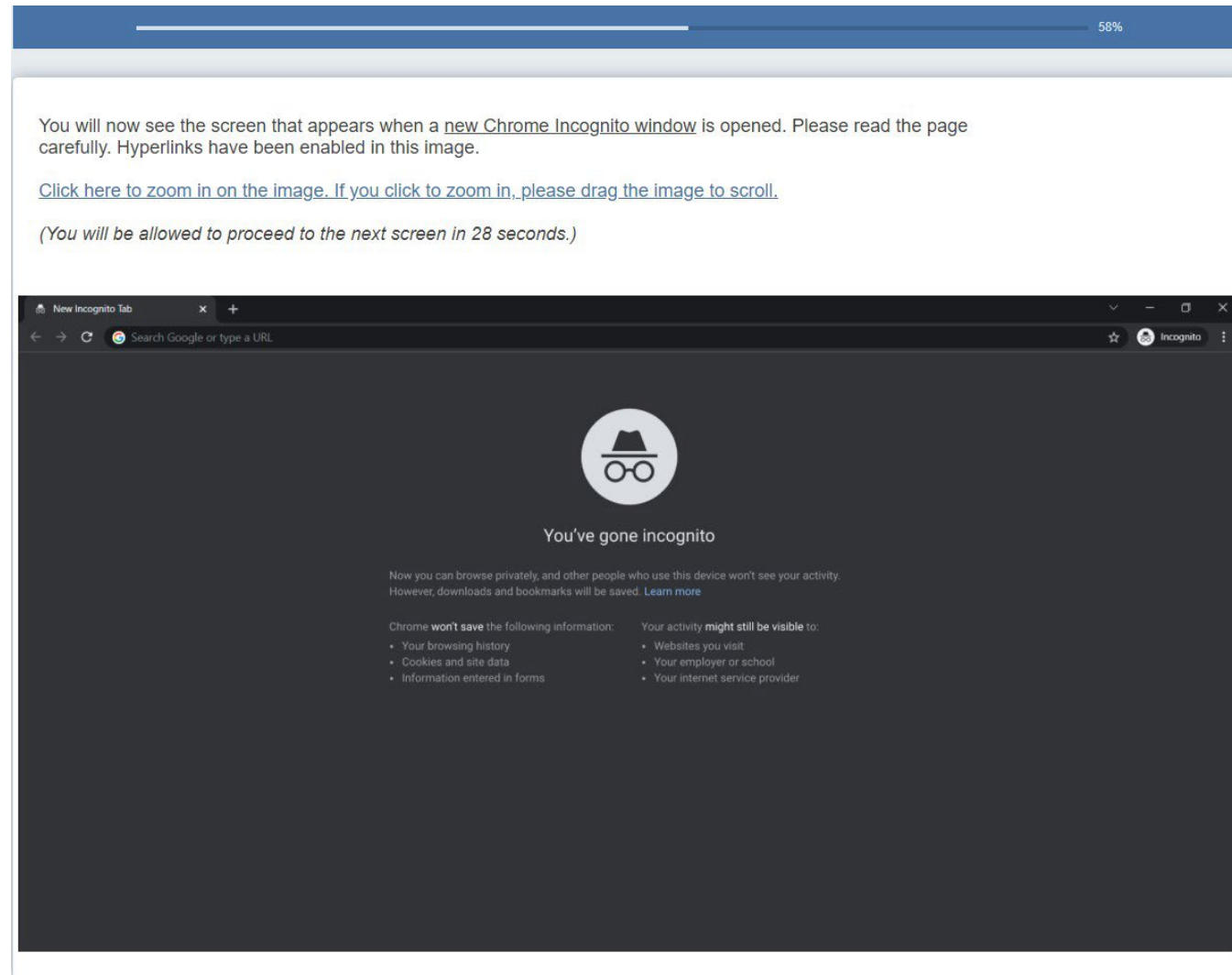
Next, you will see images of a screen that appears when you enable Chrome's Incognito mode and a page that includes additional information for private browsing, as well as Google's Privacy Policy and the Chrome Privacy Notice. Please consider these images with the intention to use private browsing mode. After, you will be asked to answer a few questions. You will be able to view these images again as you answer the questions.

Please do not use your browser's "Back" button.

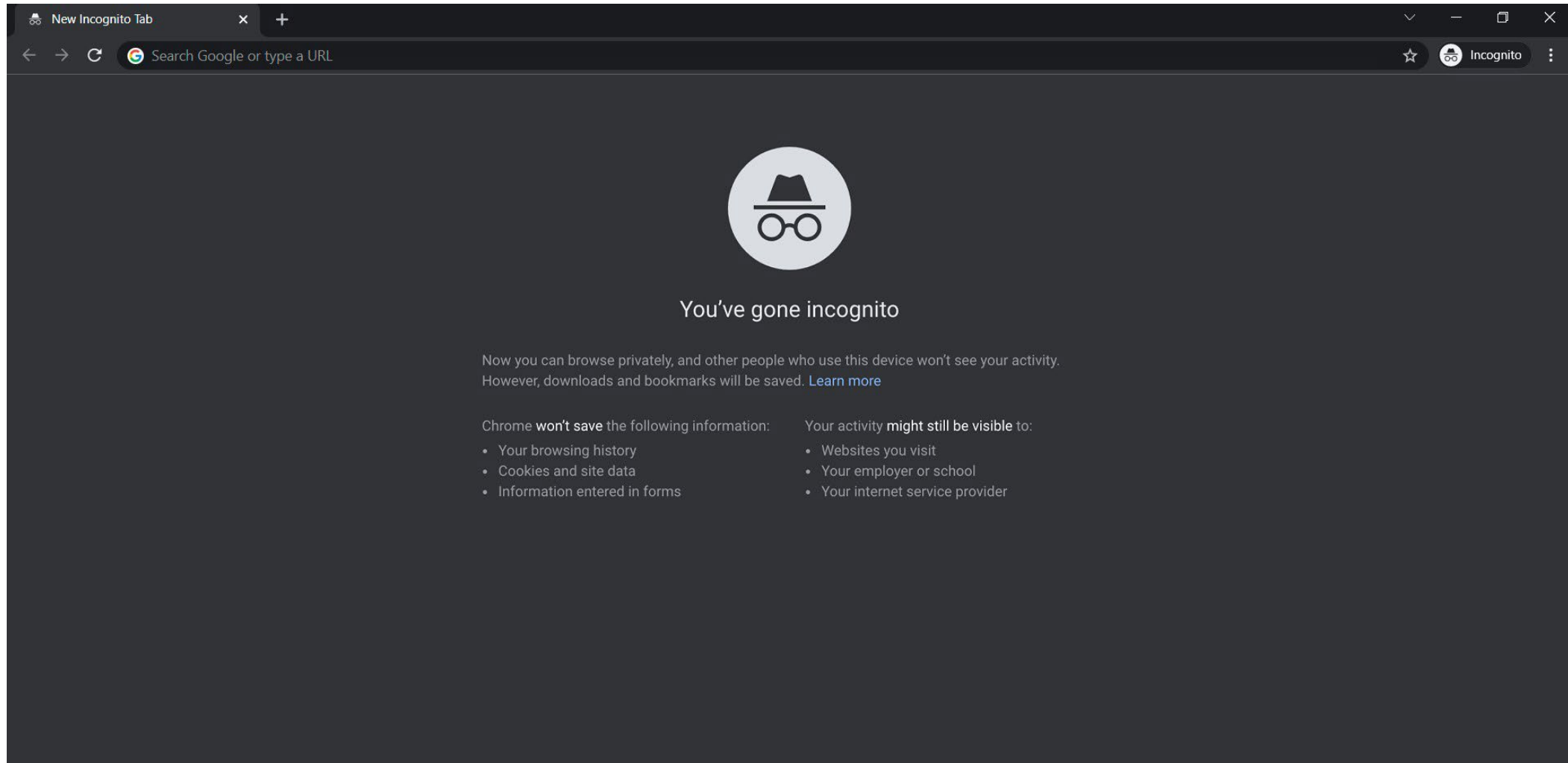
If you don't know an answer to a question or if you don't have an opinion, please don't guess. Simply indicate this in your response by selecting the "Don't know / Unsure" option or the "I don't feel I have enough information to answer this question" option. There are no right or wrong answers.

Continue





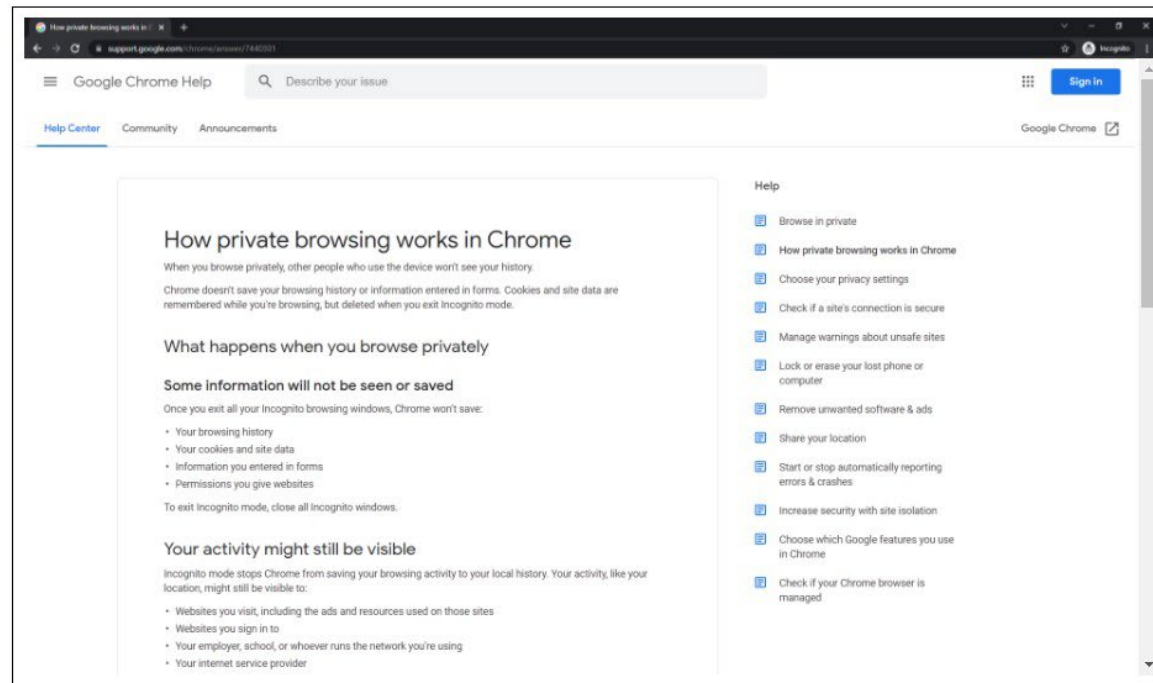
The following is the pop-up window that appears when a respondent clicks to zoom in on the previous page. The respondent can drag to navigate around the image.



You will now see the following screen that would appear if you clicked "Learn more" on the previous page. Hyperlinks and any other clickable elements in this image have been disabled.

[Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.](#)

*(You will be allowed to proceed to the next screen in 27 seconds.)*



The following is the pop-up window that appears when a respondent clicks to zoom in on the previous page. The respondent can drag to navigate around the image.

The screenshot shows the Google Chrome Help page. At the top, there is a navigation bar with the Google Chrome Help logo, a search bar with the placeholder text 'Describe your issue', and a 'Sign in' button. Below the navigation bar, there are links for 'Help Center', 'Community', and 'Announcements'. The main content area is titled 'How private browsing works in Chrome' and contains the following text:

When you browse privately, other people who use the device won't see your history.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode.

### What happens when you browse privately

#### Some information will not be seen or saved

Once you exit all your Incognito browsing windows, Chrome won't save:

- Your browsing history
- Your cookies and site data
- Information you entered in forms
- Permissions you give websites

To exit Incognito mode, close all Incognito windows.

#### Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:

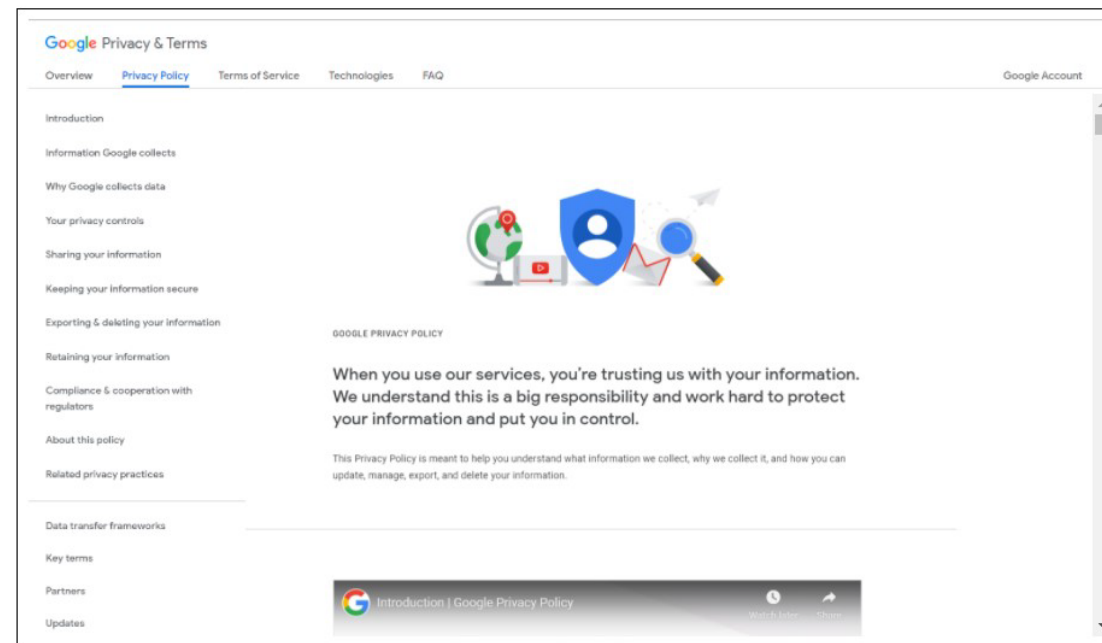
On the right side of the page, there is a 'Help' section with a list of links:

- Browse in private
- How private browsing works in Chrome
- Choose your privacy settings
- Check if a site's connection is secure
- Manage warnings about unsafe sites
- Lock or erase your lost phone or computer
- Remove unwanted software & ads
- Share your location
- Start or stop automatically reporting errors & crashes
- Increase security with site isolation
- Choose which Google features you use in Chrome
- Check if your Chrome browser is managed

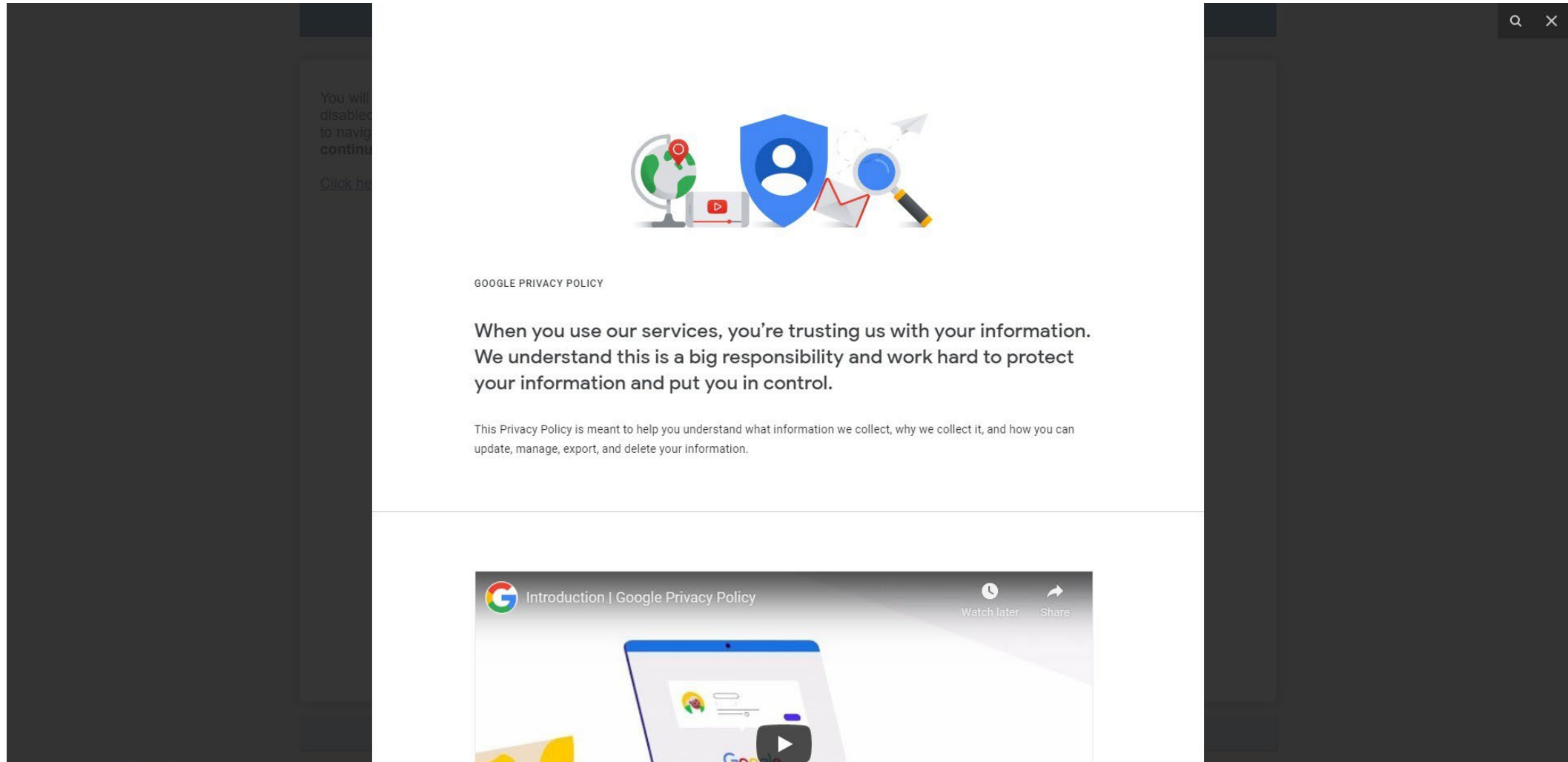
You will now see the [Google Privacy Policy](#). Please carefully read this policy. Within the policy, hyperlinks have been disabled; however, if you click on certain Table of Contents section headings on the left-hand side, you will be able to navigate to specific policy sections. **Please scroll through the window below to see the whole image. The continue button can be found at the bottom of the page.**

[Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.](#)

*(You will be allowed to proceed to the next screen in 25 seconds.)*



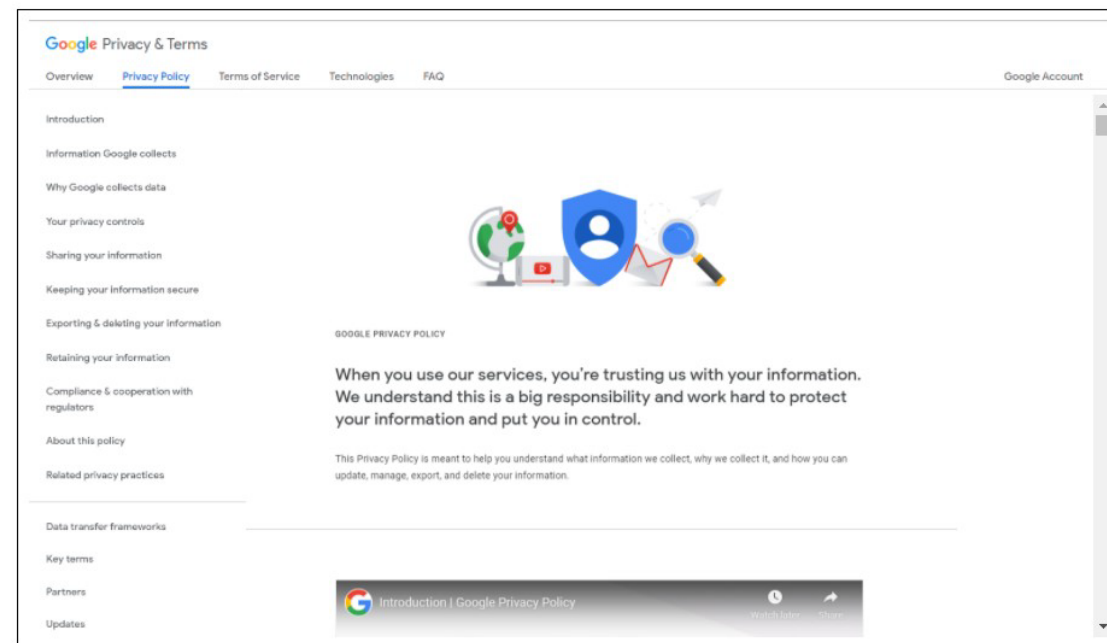
The following is the pop-up window that appears when a respondent clicks to zoom in on the previous page. The respondent can drag to navigate around the image.



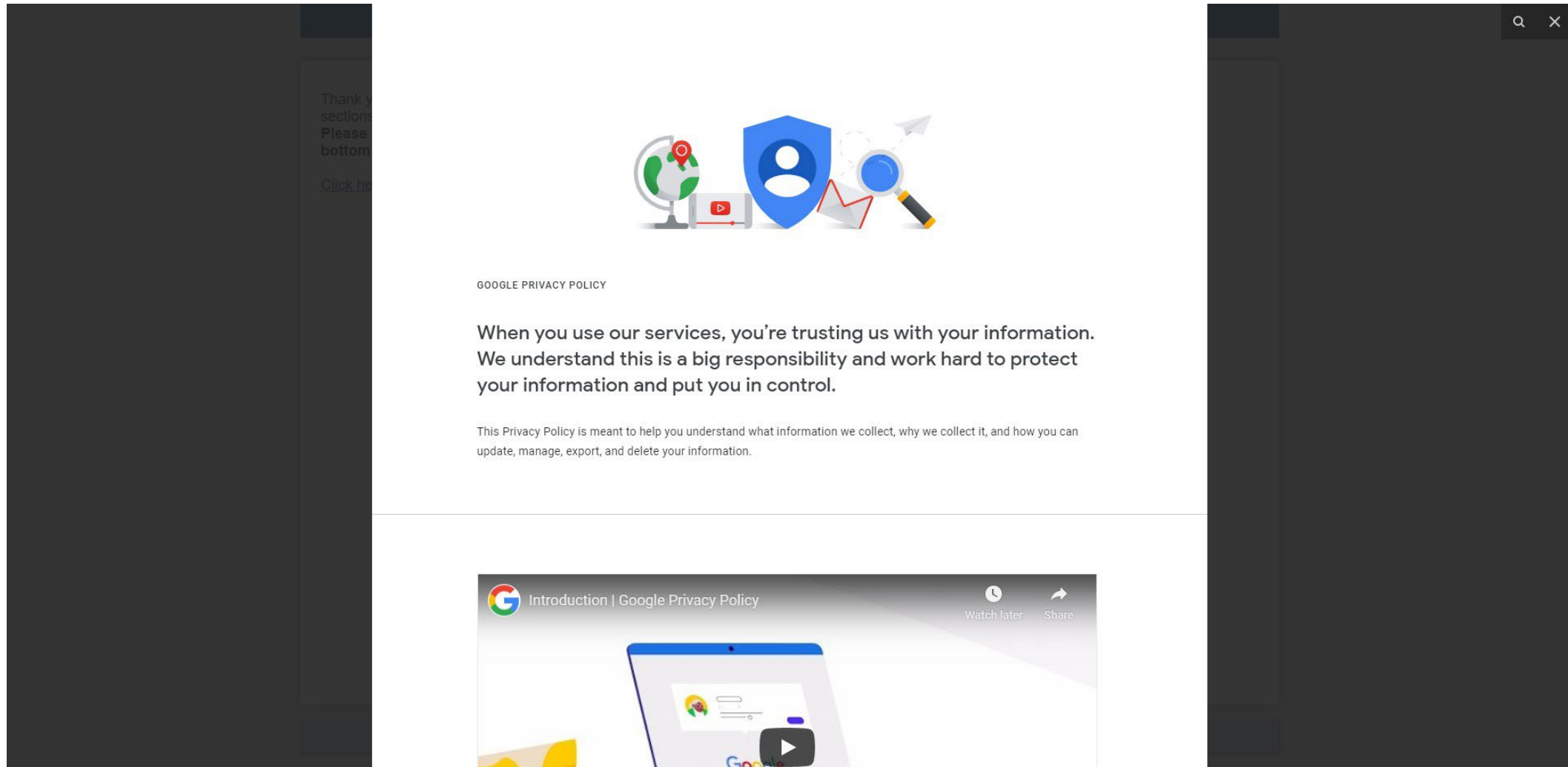
Thank you for reviewing the [Google Privacy Policy](#). Before continuing, please take another look at the highlighted sections and make sure you understand them. As you answer questions, you will be able to review the policy again. **Please scroll through the window below to see the whole image. The continue button can be found at the bottom of the page.**

[Click here to zoom in on the image. If you click to zoom in, please drag the image to scroll.](#)

*(You will be allowed to proceed to the next screen in 12 seconds.)*



The following is the pop-up window that appears when a respondent clicks to zoom in on the previous page. The respondent can drag to navigate around the image.



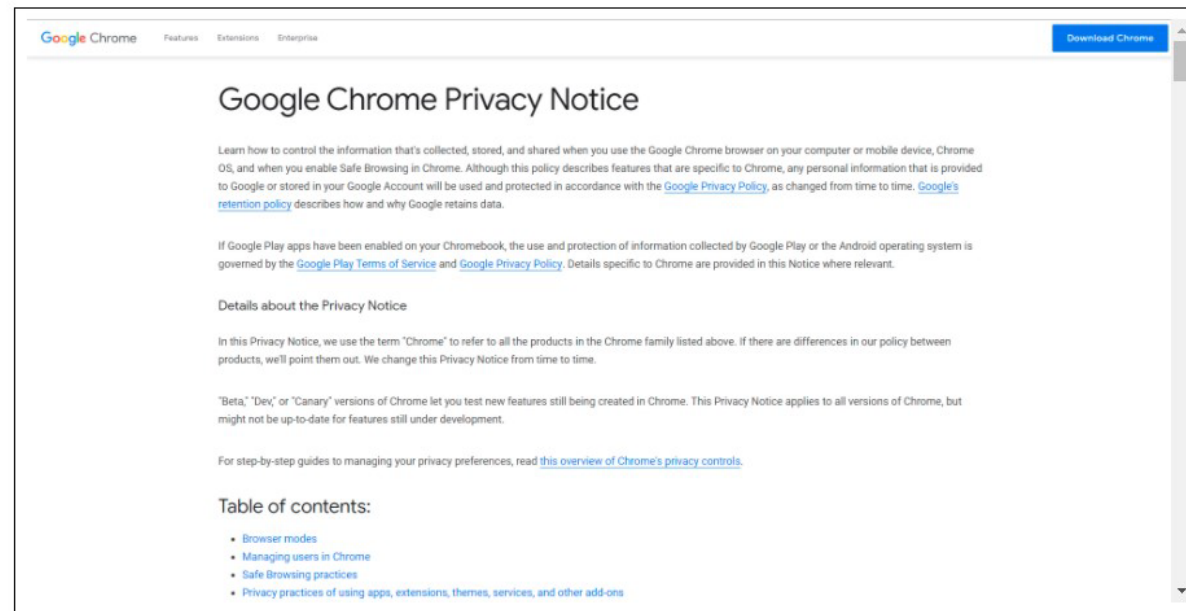
G.2-19



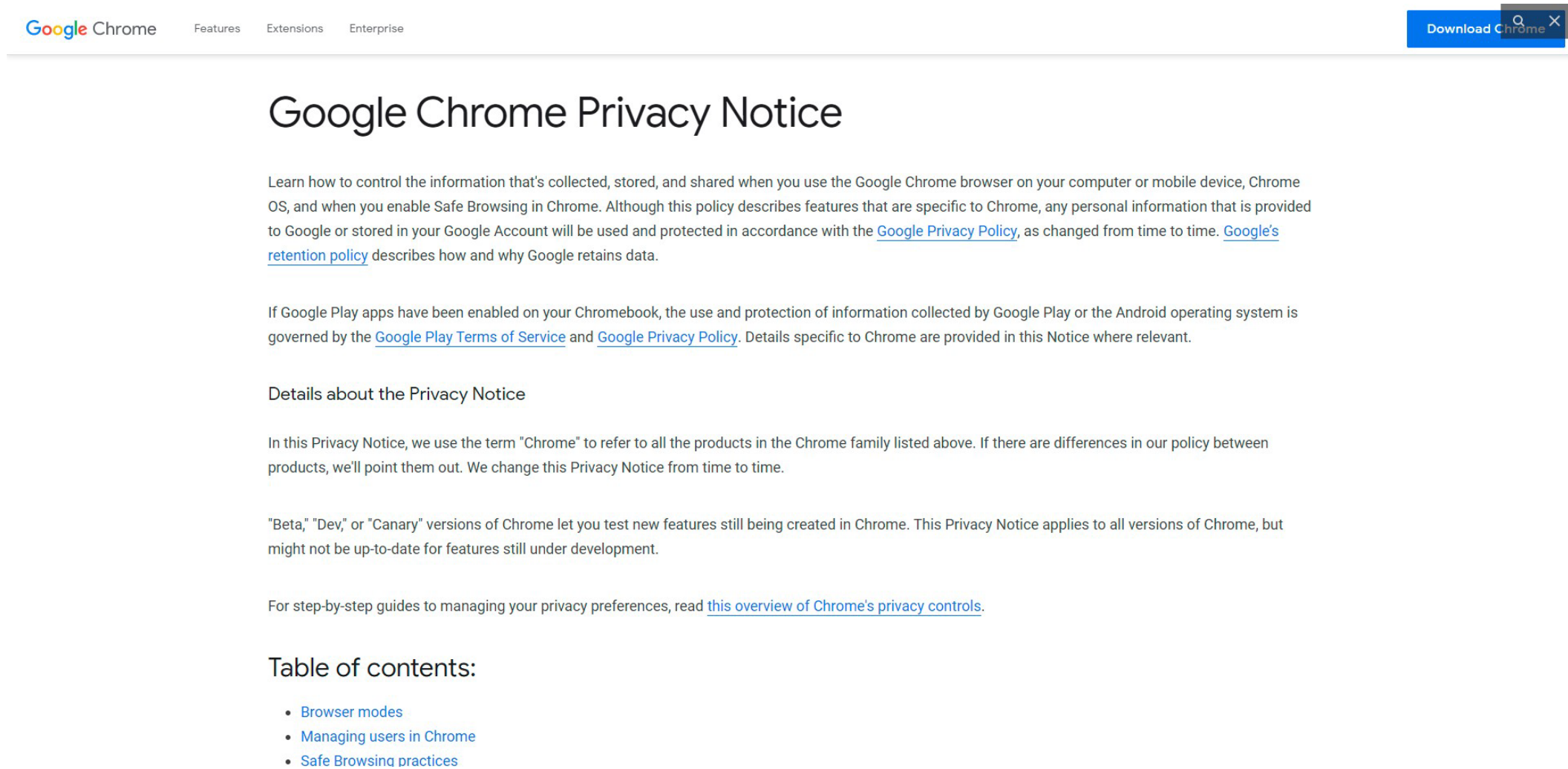
You will now see the [Chrome Privacy Notice](#). Please read it carefully. Within the policy, hyperlinks have been disabled; however, you can navigate to specific sections of the policy by clicking on the headings under the Table of Contents. **Please scroll through the window below to see the whole image. The continue button can be found at the bottom of the page.**

[Click here to zoom in on the image.](#) If you click to zoom in, please drag the image to scroll.

*(You will be allowed to proceed to the next screen in 27 seconds.)*



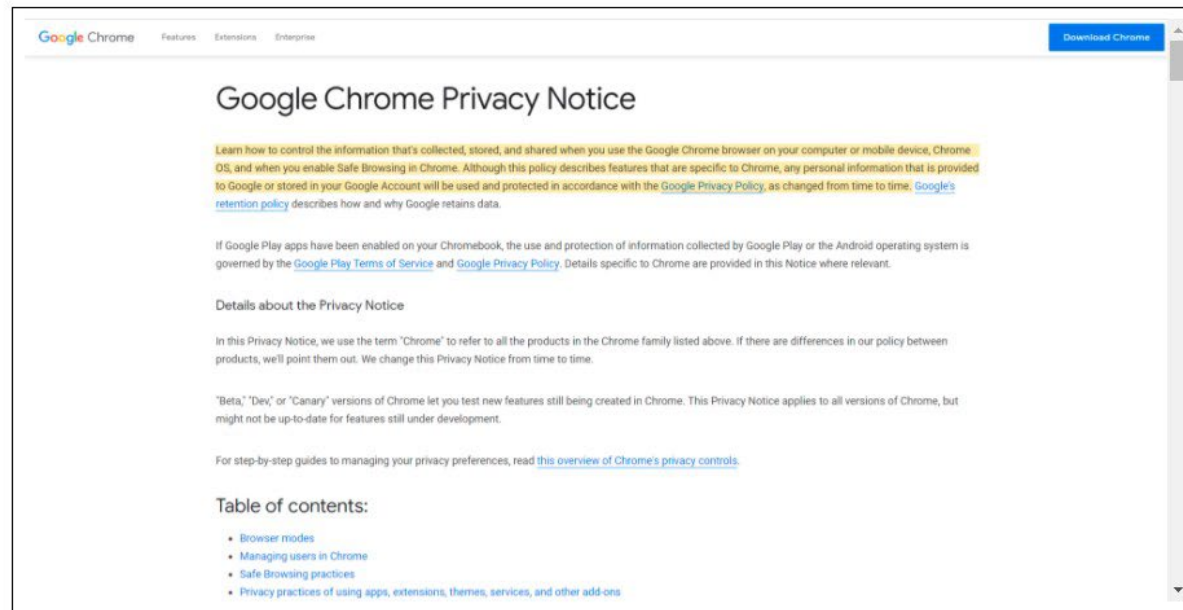
The following is the pop-up window that appears when a respondent clicks to zoom in on the previous page. The respondent can drag to navigate around the image.



Thank you for reviewing the [Chrome Privacy Notice](#). Before continuing, please take another look at the highlighted sections and make sure you understand them. As you answer questions, you will be able to review the notice again. **Please scroll through the window below to see the whole image. The continue button can be found at the bottom of the page.**

[Click here to zoom in on the image.](#) If you click to zoom in, please drag the image to scroll.

*(You will be allowed to proceed to the next screen in 11 seconds.)*



The following is the pop-up window that appears when a respondent clicks to zoom in on the previous page. The respondent can drag to navigate around the image.



# Google Chrome Privacy Notice

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read [this overview of Chrome's privacy controls](#).

## Table of contents:

- [Browser modes](#)
- [Managing users in Chrome](#)
- [Safe Browsing practices](#)

68%

(The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.)

Based on the screens that you reviewed, please select one of the following regarding [URLs of the sites you visit](#) during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product):

(Select a point on the scale. If you do not have enough information, please select "I don't feel I have enough information to answer this question")

Google does receive this information

Google probably does receive this information

It is uncertain whether Google receives this information or not

Google probably does not receive this information

Google does not receive this information

☐ I don't feel I have enough information to answer this question

[Continue](#)

72%

(The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.)

Based on the screens that you reviewed, please select one of the following regarding **IP address** during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product):  
(Select a point on the scale. If you do not have enough information, please select "I don't feel I have enough information to answer this question")

Google does receive this information





Google probably receives this information

It is uncertain whether Google receives this information or not

Google probably does not receive this information

Google does not receive this information

☐ I don't feel I have enough information to answer this question



Continue



78%

(The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.)

Based on the screens that you reviewed, please select one of the following regarding cookies placed on your browser during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product):  
(Select a point on the scale. If you do not have enough information, please select "I don't feel I have enough information to answer this question")

Google does receive this information





Google probably receives this information

It is uncertain whether Google receives this information or not

Google probably does not receive this information

Google does not receive this information

☐ I don't feel I have enough information to answer this question



Continue

84%

Were you or were you not able to view the images clearly to answer the questions asked in this survey?  
(Select only one option)

☐ I was able to view the images clearly to answer the questions asked in this survey

☐ I was not able to view the images clearly to answer the questions asked in this survey

☐ Don't know / Unsure

Continue



87%

Prior to this survey, were you or were you not aware of any lawsuits related to private browsing mode?  
(Select only one option)

☐ I was aware of at least one lawsuit related to private browsing mode

☐ I was not aware of any lawsuit related to private browsing mode

☐ Don't know / Unsure

Continue

90%

You indicated that you were aware of at least one lawsuit regarding private browsing mode. Please describe the lawsuit(s) you were aware of:

*(Please type in your response. If you do not know the answer or are unsure, please select "Don't know / Unsure")*

☐ Don't know / Unsure

Continue

92%

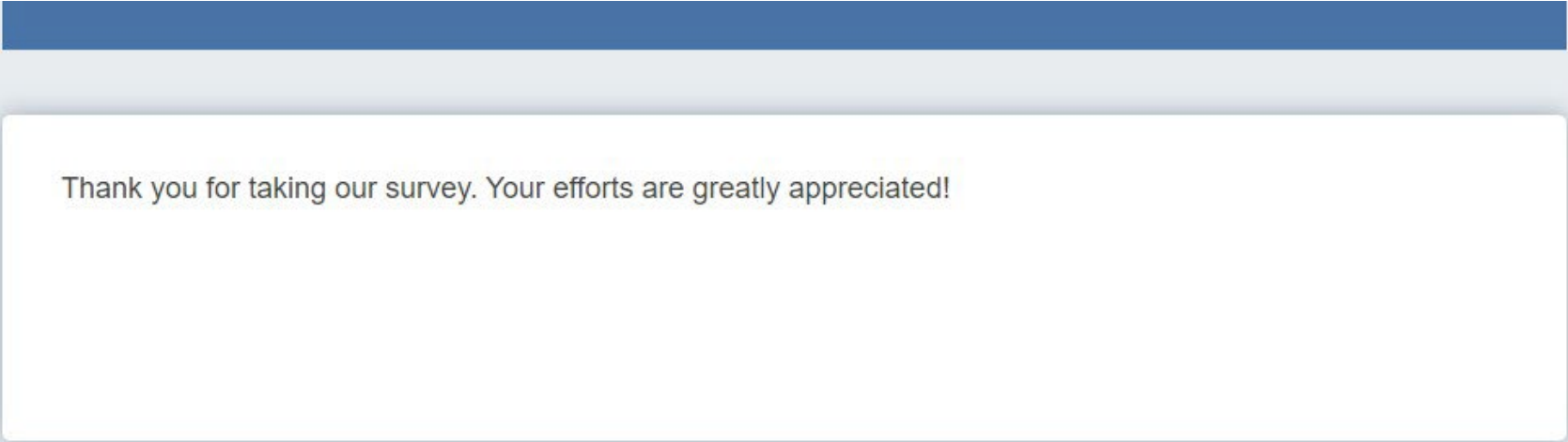
In the past three months, have you or have you not taken any other survey related to private browsing mode?  
(Select only one option)

☐ I have taken a survey related to private browsing mode

☐ I have not taken a survey related to private browsing mode

☐ Don't know / Unsure

Continue



Thank you for taking our survey. Your efforts are greatly appreciated!

**APPENDIX G.3**

**LIKELIHOOD OF USE**

**SURVEY SCREENSHOTS**

**(ACTUAL LANGUAGE**

**GROUP)**

0%

Please enter the code exactly as it appears in the image below and then click "Continue" to continue.

YL2QRF

Continue

3%

Thank you for participating in our study. Your opinions are very important to us. If you don't know an answer to a question or if you don't have an opinion, please don't guess. Simply indicate this in your response by selecting the "Don't know / Unsure" option or the "I don't feel I have enough information to answer this question" option. There are no right or wrong answers.

Your answers will be kept in strict confidence and the results of this study will not be used to try to sell you anything. Trademarks and logos are all the intellectual property of their respective owners.

If you wear glasses or corrective lenses when using a desktop computer, laptop computer, mobile phone, or tablet, please wear them throughout the survey.

Please do not use the "Back" button of your browser while taking the survey. This survey will take less than 15 minutes of your time. When you are ready to get started, please select the "Continue" button.

Continue

6%

What is your age?

*(Select only one option)*

☐ 60 or older

☐ 50 – 59

☐ 40 – 49

☐ 30 – 39

☐ 18 – 29

☐ Under 18

☐ Prefer not to answer

Continue



9%

Are you...?

*(Select only one option)*

☐ Male

☐ Female

☐ Other

☐ Prefer not to answer

Continue

13%

In which state do you live?

*(Select only one option)*

Select one... ▼

☐ Prefer not to answer

☐ Don't know / Unsure

Continue

19%

Have you or any member of your household ever worked for any of the following types of companies?  
(Select all that apply)

☐ A technology company or technology consultancy

☐ A real estate agency

☐ A construction company

☐ A healthcare provider or medical office

☐ An academic institution

☐ A clothing retailer

☐ A fitness center

☐ A marketing, market research, or advertising agency

☐ A law firm, legal services organization, or court

☐ A car dealership

☐ None of the above

Continue

26%

This question is to check your attention. Please select “South” from the answer options below.  
(Select only one option)

☐ South

☐ North

☐ West

☐ East

☐ None of the above

☐ Don't know / Unsure

Continue

30%

Thinking about the device(s) you use to browse the internet (such as your phone, your personal laptop, or your office computer), which internet browser(s) do you currently use?  
(Select all that apply)

☐ Google Chrome

☐ Mozilla Firefox

☐ Microsoft Edge

☐ DuckDuckGo

☐ Safari

☐ Internet Explorer

☐ Brave

☐ Odeon

☐ Opera

☐ Other (Please specify)

☐ Don't know / Unsure

Continue

41%

In the past six months, which of the following features, if any, have you used on your internet browser(s)?  
(Select all that apply)

☐ Bookmarks

☐ Screenshot tool

☐ Customized home page

☐ Website translator

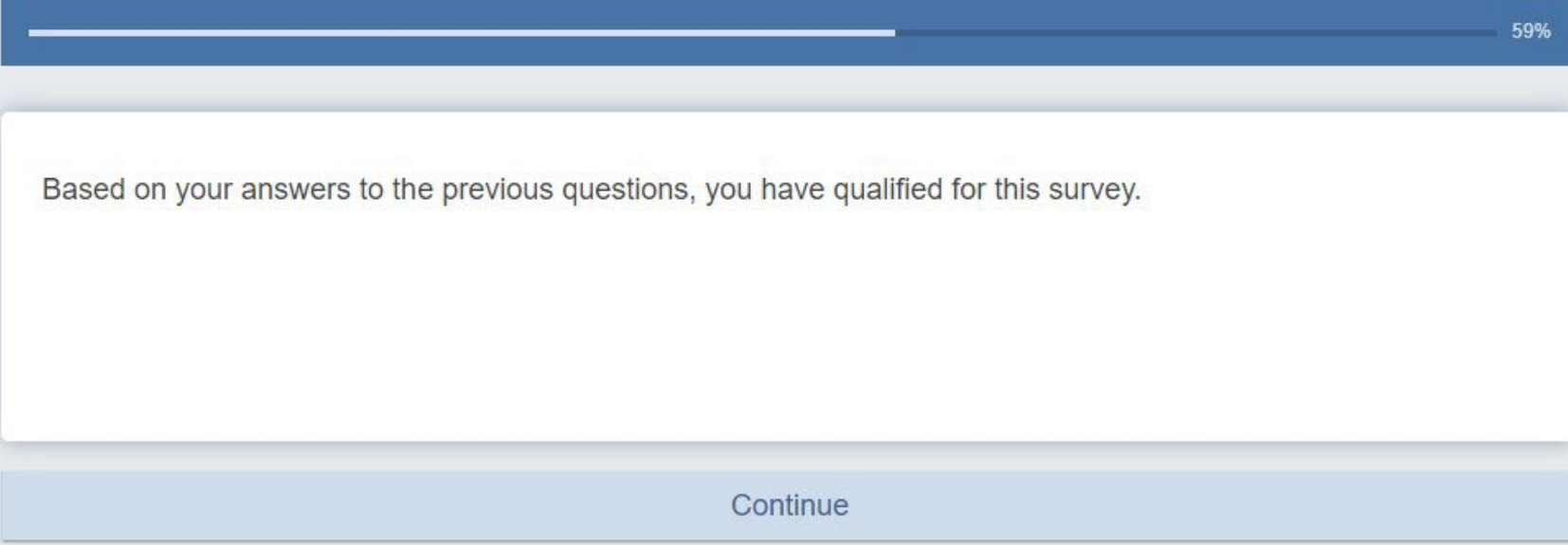
☐ Dark mode for visual display

☐ Private browsing mode

☐ Other (Please specify)

☐ Don't know / Unsure

Continue



A survey progress bar at the top shows 59% completion. Below it, a white box contains the text: "Based on your answers to the previous questions, you have qualified for this survey." At the bottom is a light blue button labeled "Continue".

59%

Based on your answers to the previous questions, you have qualified for this survey.

Continue

63%

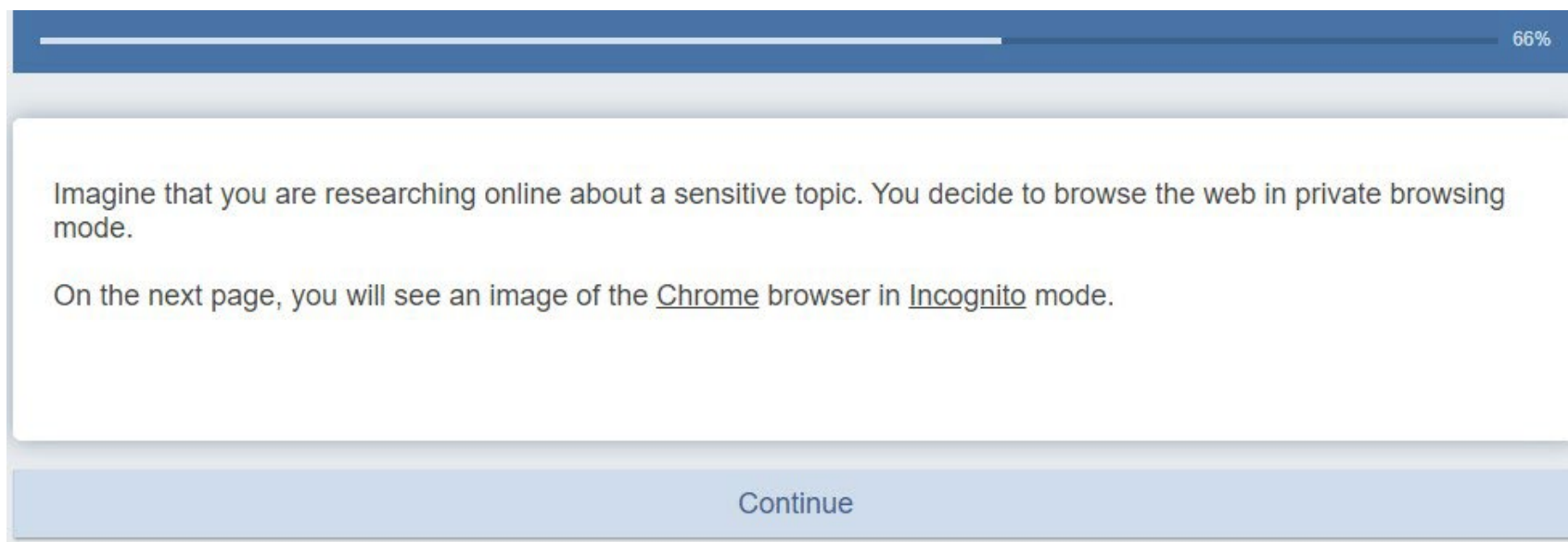
You will first be presented with a scenario. Next, you will see an image. After, you will be asked to answer a few questions. You will be able to view any images again as you answer the questions.

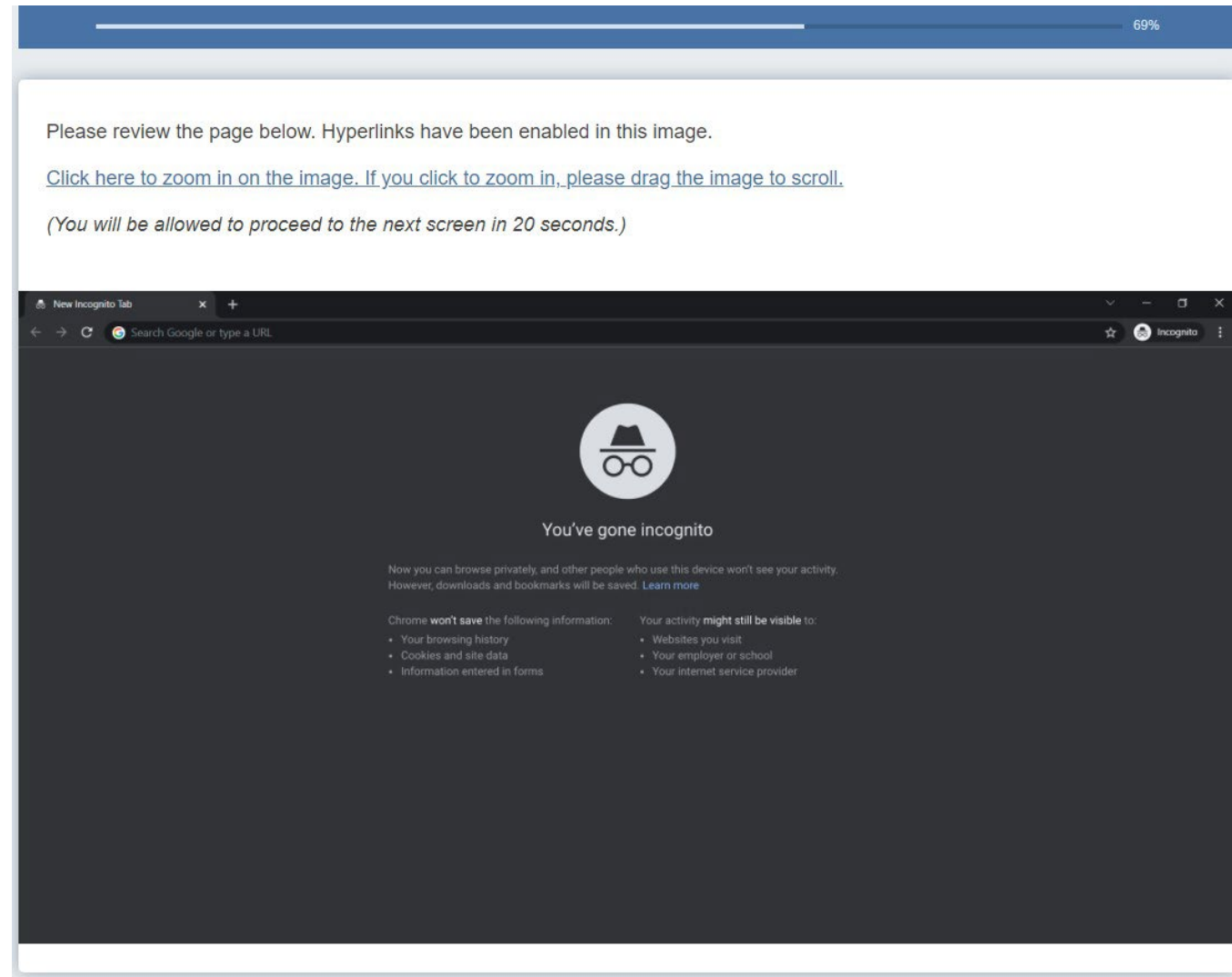
Please do not use your browser's "Back" button.

If you don't know an answer to a question or if you don't have an opinion, please don't guess. Simply indicate this in your response by selecting the "Don't know / Unsure" option or the "I don't feel I have enough information to answer this question" option. There are no right or wrong answers.

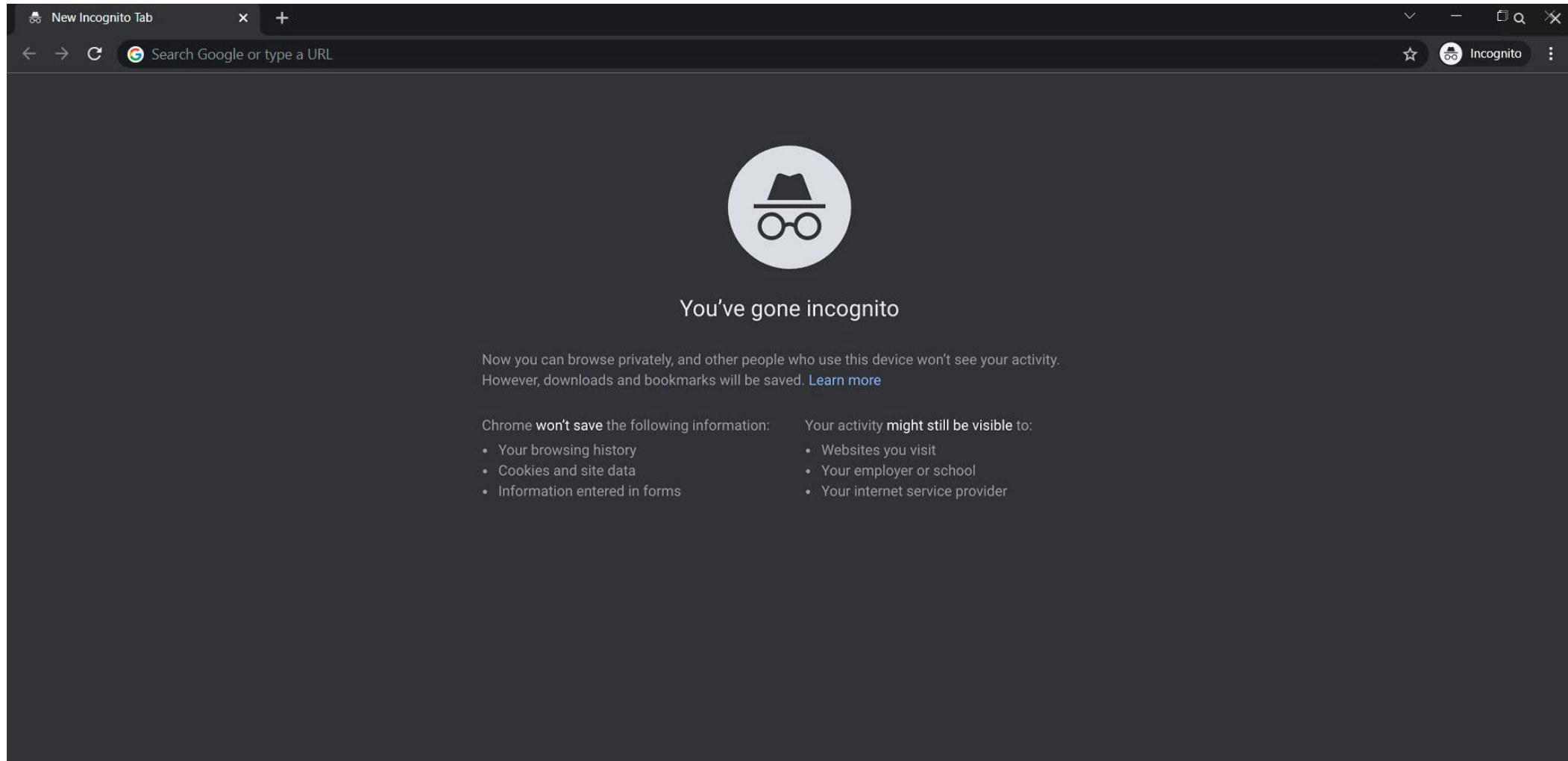
Continue

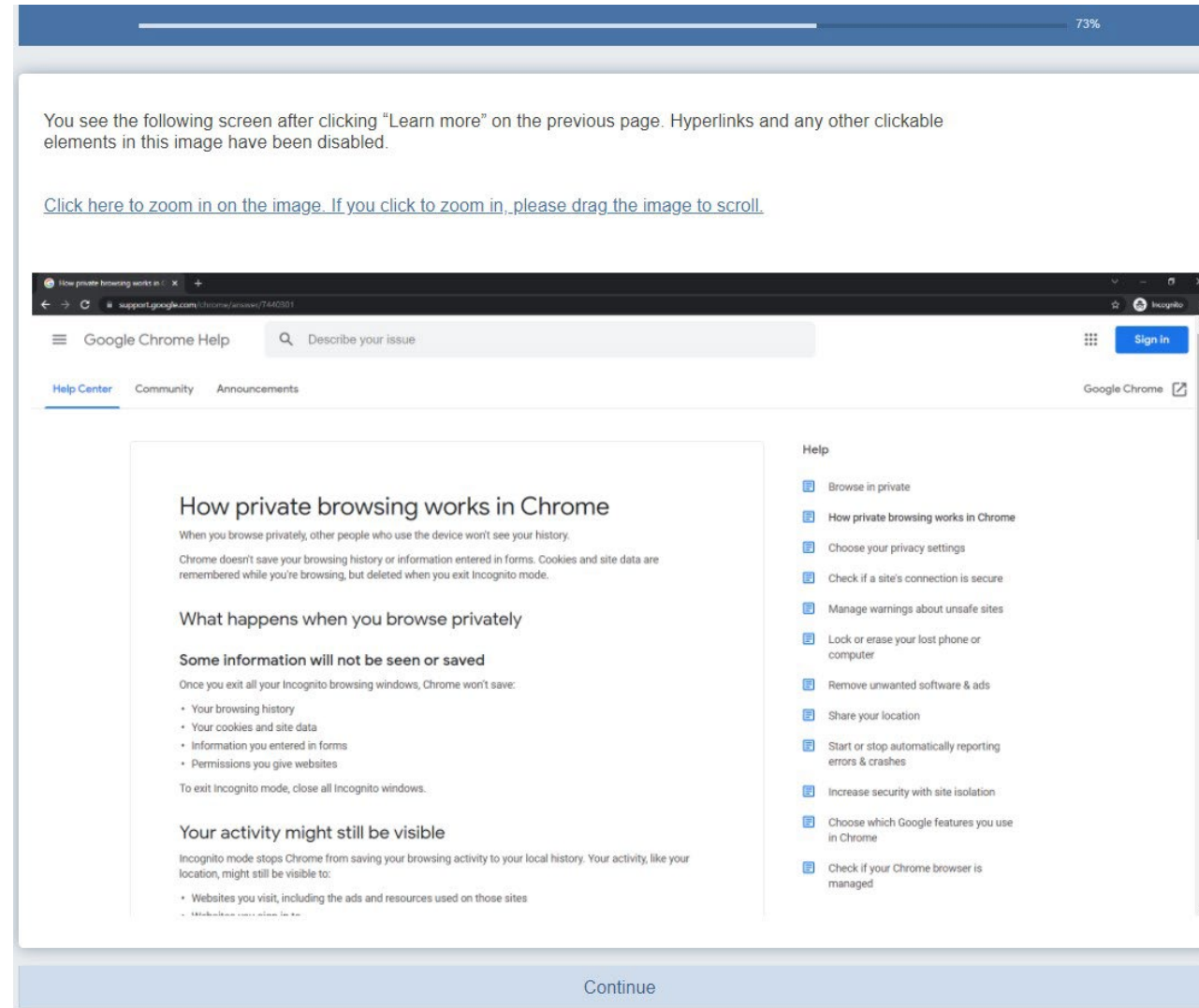






The following is the pop-up window that appears when a respondent clicks to zoom in on the previous page. The respondent can drag to navigate around the image.





The following is the pop-up window that appears when a respondent clicks to zoom in on the previous page. The respondent can drag to navigate around the image.

The screenshot shows the Google Chrome Help page. At the top, there is a navigation bar with the Google Chrome Help logo, a search bar with the placeholder text 'Describe your issue', and a 'Sign in' button. Below the navigation bar, there are links for 'Help Center', 'Community', and 'Announcements'. The main content area is titled 'How private browsing works in Chrome' and contains the following text:

When you browse privately, other people who use the device won't see your history.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode.

### What happens when you browse privately

#### Some information will not be seen or saved

Once you exit all your Incognito browsing windows, Chrome won't save:

- Your browsing history
- Your cookies and site data
- Information you entered in forms
- Permissions you give websites

To exit Incognito mode, close all Incognito windows.

#### Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:

On the right side of the page, there is a 'Help' section with a list of links:

- Browse in private
- How private browsing works in Chrome
- Choose your privacy settings
- Check if a site's connection is secure
- Manage warnings about unsafe sites
- Lock or erase your lost phone or computer
- Remove unwanted software & ads
- Share your location
- Start or stop automatically reporting errors & crashes
- Increase security with site isolation
- Choose which Google features you use in Chrome
- Check if your Chrome browser is managed

73%



(The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.)

How likely or unlikely are you to use the Chrome browser in Incognito mode for your online research about the sensitive topic mentioned in the previous scenario?

(Select a point on the scale. If you do not have enough information, please select "I don't feel I have enough information to answer this question.")

Likely to use the Chrome browser in Incognito mode      Somewhat likely to use the Chrome browser in Incognito mode      Neither likely nor unlikely to use the Chrome browser in Incognito mode      Somewhat unlikely to use the Chrome browser in Incognito mode      Unlikely to use the Chrome browser in Incognito mode

☐ I don't feel I have enough information to answer this question

Continue

77%

Were you or were you not able to view the images clearly to answer the questions asked in this survey?  
(Select only one option)

☐ I was not able to view the images clearly to answer the questions asked in this survey

☐ I was able to view the images clearly to answer the questions asked in this survey

☐ Don't know / Unsure

Continue

84%

Prior to this survey, were you or were you not aware of any lawsuits related to private browsing mode?  
(Select only one option)

☐ I was not aware of any lawsuit related to private browsing mode

☐ I was aware of at least one lawsuit related to private browsing mode

☐ Don't know / Unsure

Continue



87%

You indicated that you were aware of at least one lawsuit regarding private browsing mode. Please describe the lawsuit(s) you were aware of:

*(Please type in your response. If you do not know the answer or are unsure, please select "Don't know / Unsure")*

☐ Don't know / Unsure

Continue

90%

In the past three months, have you or have you not taken any other survey related to private browsing mode?  
(Select only one option)

☐ I have not taken a survey related to private browsing mode

☐ I have taken a survey related to private browsing mode

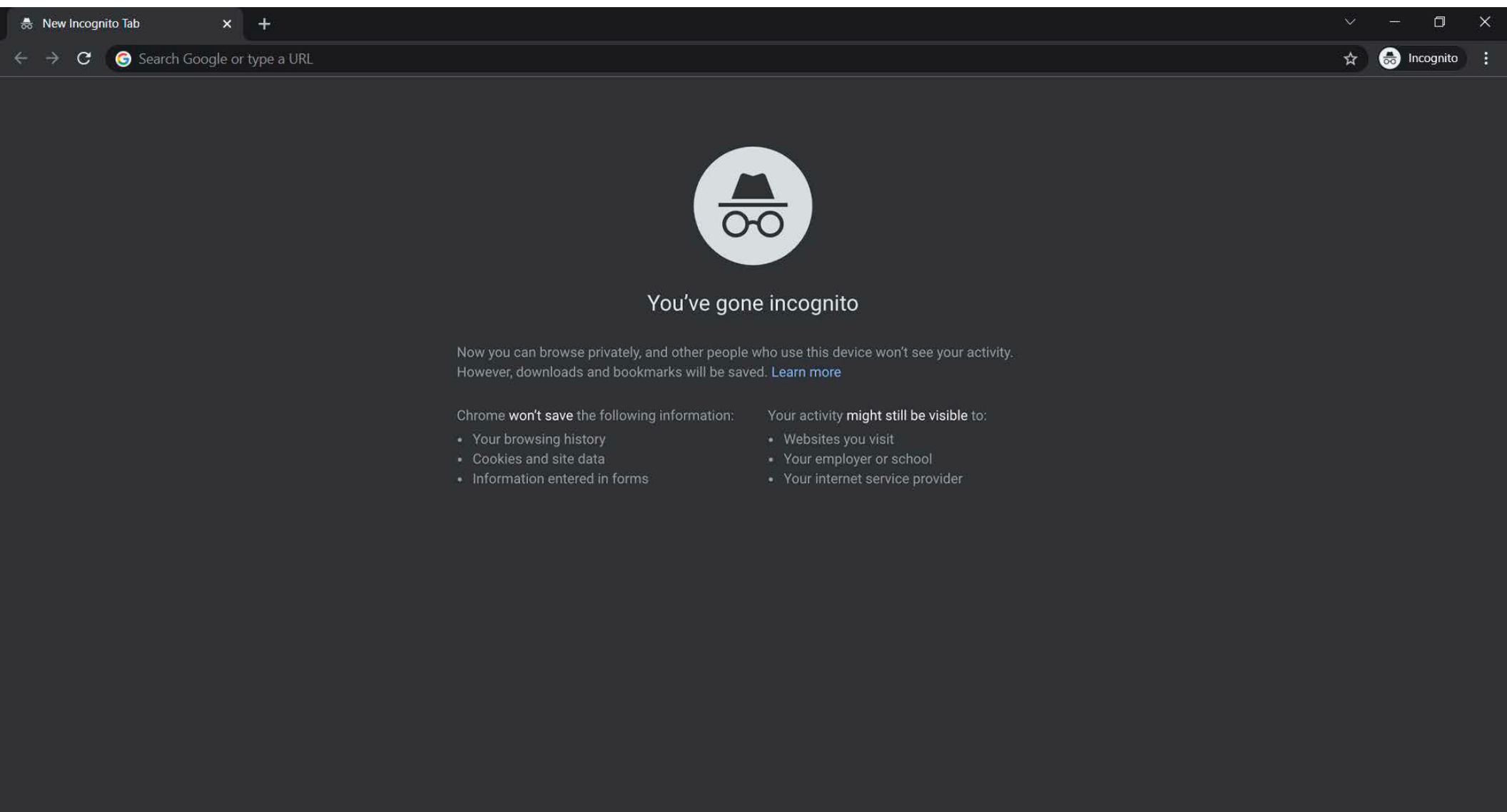
☐ Don't know / Unsure

Continue



Thank you for taking our survey. Your efforts are greatly appreciated!

**APPENDIX H.1**  
**CHROME**  
**INCOGNITO SPLASH SCREEN**  
**(ACTUAL LANGUAGE)**



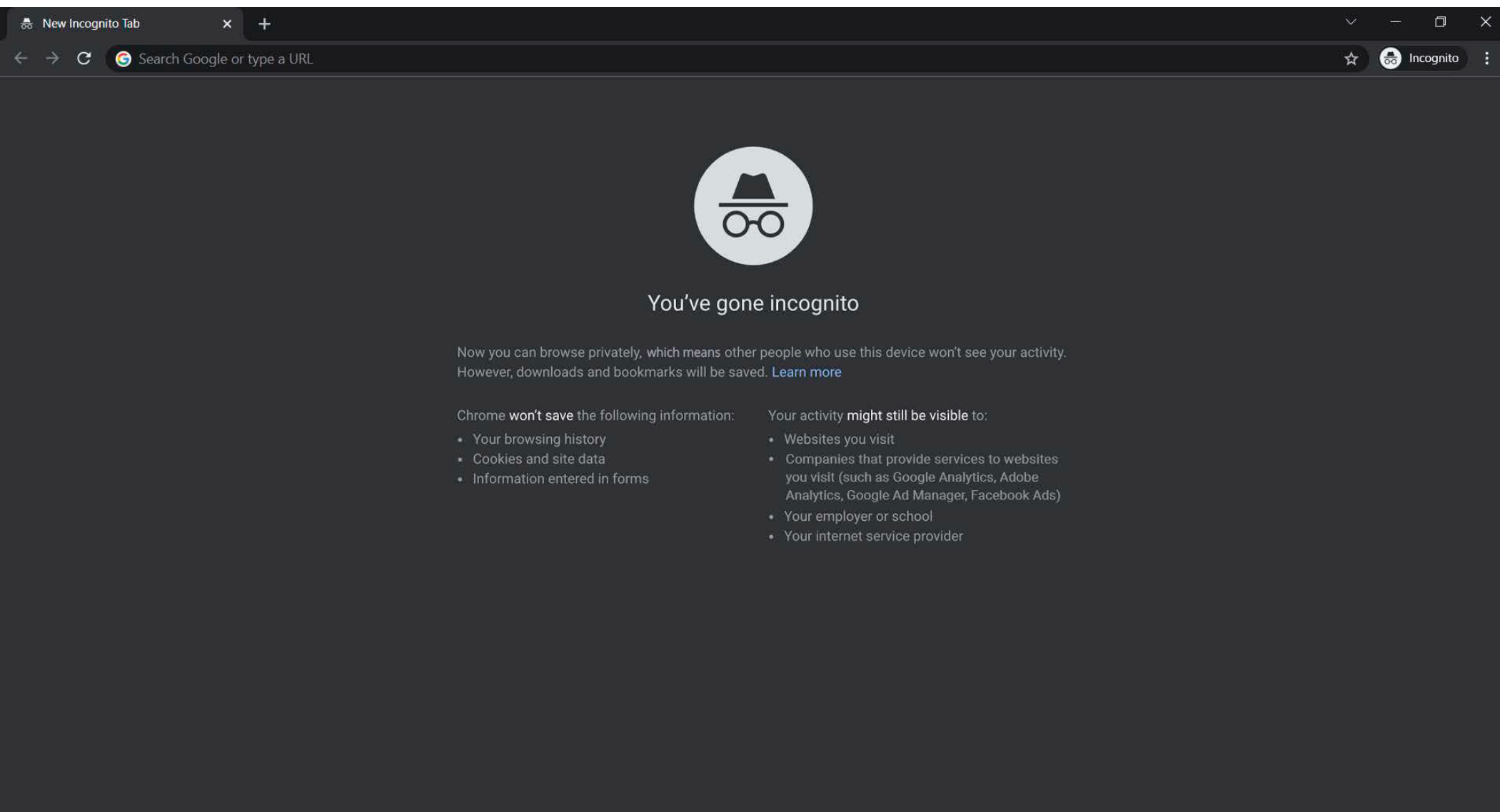
**APPENDIX H.2**

**CHROME**

**INCOGNITO SPLASH**

**SCREEN (ALTERNATIVE**

**LANGUAGE)**



**APPENDIX I.1**  
**CHROME**  
**“LEARN MORE” PAGE**  
**(ACTUAL LANGUAGE)**



Google Chrome Help

Describe your issue

Sign in

[Help Center](#)
[Community](#)
[Announcements](#)

Google Chrome

## How private browsing works in Chrome

When you browse privately, other people who use the device won't see your history.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode.

### What happens when you browse privately

#### Some information will not be seen or saved

Once you exit all your Incognito windows, Chrome won't save:

- Your browsing history
- Your cookies and site data
- Information you entered in forms
- Permissions you give websites

To exit Incognito mode, close all Incognito windows.

#### Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:

- Websites you visit, including the ads and resources used on those sites
- Websites you sign in to
- Your employer, school, or whoever runs the network you're using
- Your internet service provider
- Search engines
  - Search engines may show search suggestions based on your location or activity in your current Incognito browsing session.

#### Some of your info might still be visible

A web service, website, search engine, or provider may be able to see:

- Your IP address, which can be used to identify your general location
- Your activity when you use a web service
- Your identity if you sign in to a web service, like Gmail

You can still find and use your payment, password and contact info, but you can't change your saved info in a Chrome Incognito window.

#### Downloads and bookmarks are saved

Chrome won't store the files you download while browsing in private. But, they're still saved to your Downloads folder, even after you exit Incognito. You and anyone who uses your device can see and open the files.

All bookmarks you create are saved to Chrome.

Some of your preferences, including accessibility choices and bookmark settings, may also be saved to Chrome.

[Computer](#)
[Android](#)
[iPhone & iPad](#)

You can switch between Incognito windows and regular Chrome windows. You'll only browse in private when you're using an Incognito window.

### Close Incognito mode to stop private browsing

Incognito mode runs in a separate window from your normal Chrome windows.

If you have an Incognito window open and you open another one, your private browsing session will continue in the new window. To exit Incognito mode, close all Incognito windows.

If you see a number next to the Incognito icon at the top right, you have more than one Incognito window open. To close an Incognito window:

- On your computer, go to your Incognito window.
- Close the window:
  - Windows or Chrome OS:** At the top right, click Close .
  - Mac:** At the top left, click Close .

### Related articles

- [Browse in private](#)
- [Let others browse Chrome as a guest](#)
- [Clear Chrome browsing data](#)

Was this helpful?

Yes
No

### Help

- [Browse in private](#)
- [How private browsing works in Chrome](#)
- [Choose your privacy settings](#)
- [Check if a site's connection is secure](#)
- [Manage warnings about unsafe sites](#)
- [Lock or erase your lost phone or computer](#)
- [Remove unwanted software & ads](#)
- [Share your location](#)
- [Start or stop automatically reporting errors & crashes](#)
- [Increase security with site isolation](#)
- [Choose which Google features you use in Chrome](#)
- [Check if your Chrome browser is managed](#)

[Watch video tutorials](#)

To get the latest tips, tricks, and how-to's, [subscribe to our YouTube Channel](#).

©2020 Google - [Privacy Policy](#) - [Terms of Service](#)

English

[Send feedback about our Help Center](#)

**APPENDIX I.2**  
**CHROME**  
**“LEARN MORE” PAGE**  
**(ALTERNATIVE LANGUAGE)**

Google Chrome Help

Describe your issue



Sign in

[Help Center](#) [Community](#) [Announcements](#)

Google Chrome

## How private browsing works in Chrome

When you browse privately, other people who use the device won't see your history.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode.

### What happens when you browse privately

#### Some information will not be seen or saved

Once you exit all your Incognito browsing windows, Chrome won't save:

- Your browsing history
- Your cookies and site data
- Information you entered in forms
- Permissions you give websites

To exit Incognito mode, close all Incognito windows.

#### Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:

- Websites you visit, including the ads and resources used on those sites (such as Google Analytics, Adobe Analytics, Google Ad Manager, Facebook Ads)
- Websites you sign in to
- Your employer, school, or whoever runs the network you're using
- Your internet service provider
- Search engines
  - Search engines may show search suggestions based on your location or activity in your current Incognito browsing session.

#### Some of your info might still be visible

A web service (such as Google Analytics, Adobe Analytics, Google Ad Manager, Facebook Ads), website, search engine, or provider may be able to see:

- Your IP address, which can be used to identify your general location
- Your activity when you use a web service
- Your identity if you sign in to a web service, like Gmail

You can still find and use your payment, password and contact info, but you can't change your saved info in a Chrome Incognito window.

#### Downloads and bookmarks are saved

Chrome won't store the files you download while browsing in private. But, they're still saved to your Downloads folder, even after you exit Incognito. You and anyone who uses your device can see and open the files.

All bookmarks you create are saved to Chrome.

Some of your preferences, including accessibility choices and bookmark settings, may also be saved to Chrome.

[Computer](#) [Android](#) [iPhone & iPad](#)

You can switch between Incognito windows and regular Chrome windows. You'll only browse in private when you're using an Incognito window.

### Close Incognito mode to stop private browsing

Incognito mode runs in a separate window from your normal Chrome windows.

If you have an Incognito window open and you open another one, your private browsing session will continue in the new window. To exit Incognito mode, close all Incognito windows.

If you see a number next to the Incognito icon at the top right, you have more than one Incognito window open. To close an Incognito window:

1. On your computer, go to your Incognito window.
2. Close the window:
  - **Windows or Chrome OS:** At the top right, click Close
  - **Mac:** At the top left, click Close

### Related articles

- [Browse in private](#)
- [Let others browse Chrome as a guest](#)
- [Clear Chrome browsing data](#)

Was this helpful?

[Yes](#)[No](#)

#### Help

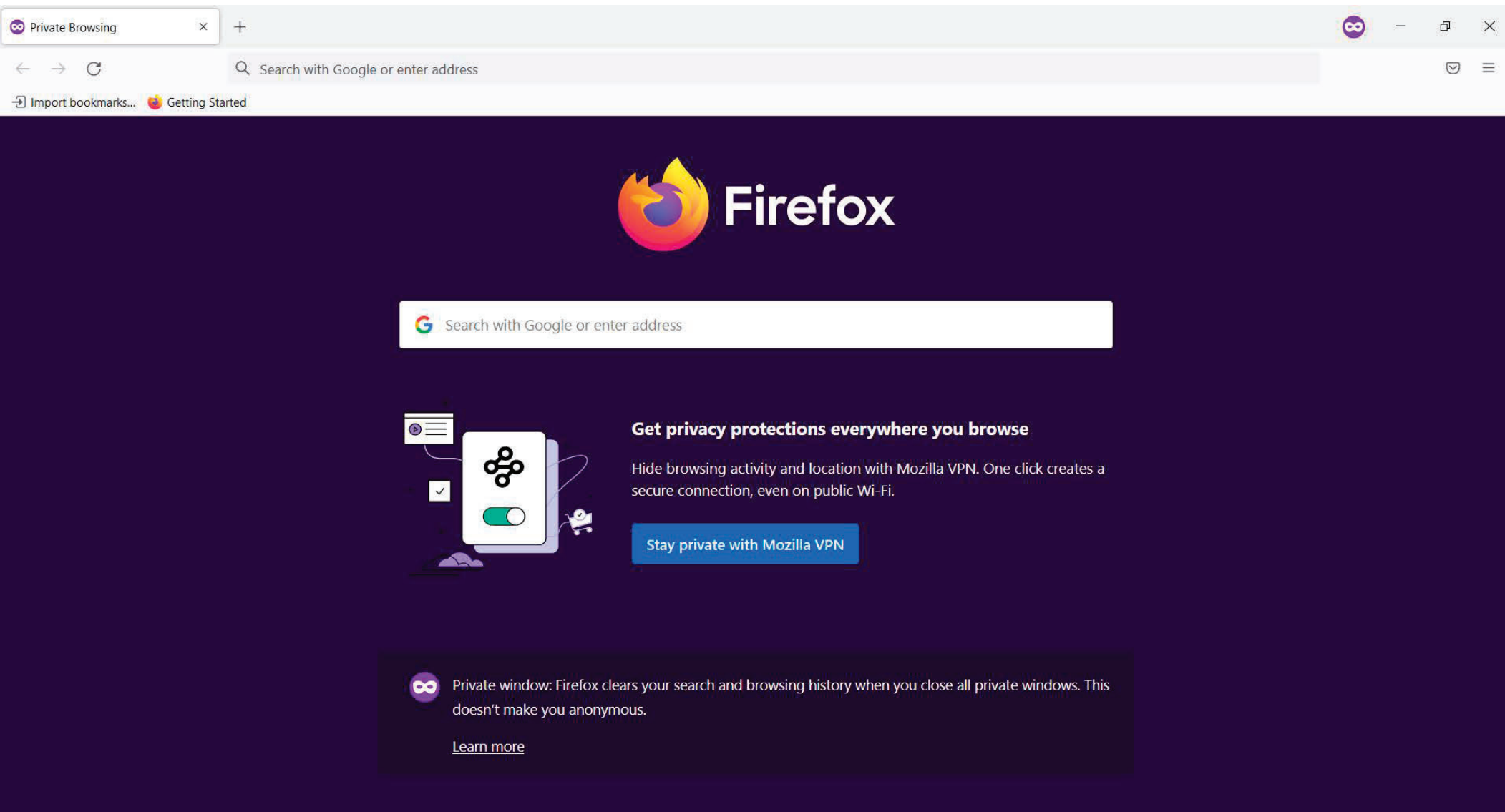
- [Browse in private](#)
- [How private browsing works in Chrome](#)
- [Choose your privacy settings](#)
- [Check if a site's connection is secure](#)
- [Manage warnings about unsafe sites](#)
- [Lock or erase your lost phone or computer](#)
- [Remove unwanted software & ads](#)
- [Share your location](#)
- [Start or stop automatically reporting errors & crashes](#)
- [Increase security with site isolation](#)
- [Choose which Google features you use in Chrome](#)
- [Check if your Chrome browser is managed](#)

[Watch video tutorials](#)

To get the latest tips, tricks, and how-tos, subscribe to our YouTube Channel.

[Send feedback about our Help Center](#)

**APPENDIX J**  
**FIREFOX**  
**PRIVATE BROWSING**  
**SPLASH SCREEN**



**APPENDIX K**  
**FIREFOX**  
**“LEARN MORE” PAGE**



Get Help

Volunteer

Sign In/Up

Home / Firefox / Protect your privacy / Common Myths about Private Browsing

Find help...



Download Firefox

[Systems and Languages](#) [What's New](#) [Privacy](#)

# Common Myths about Private Browsing

## Customize this article

☒ Firefox

Version 95

Windows 10

[Private Browsing](#) is a useful feature of Firefox, but only if you understand the protection it offers. It helps you obscure your online activity from other people who use Firefox on your computer, but does not make you invisible online.

### Myth 1: Private Browsing makes you anonymous on the Internet.

**Reality:** Private Browsing does not mask your identity or activity online. Websites and Internet service providers can still gather information about your visit, even if you are not signed in. If you use your device at work, your company may be able to monitor the websites you visit. If you surf the Web at home, your cable company (or their partners) may have access to your browsing information. Only a [Virtual Private Network \(VPN\)](#) can mask your location and encrypt your online activity, keeping your identity and data safe from prying eyes. If you need to stay anonymous online, try [Mozilla VPN](#).

### Myth 2: Private Browsing removes all traces of your browsing activity from your computer.

**Reality:** Private Browsing works by letting you browse without saving passwords, cookies and browsing history in a Private Window. If you download a file from a website, it will remain on your computer, but it will not appear in the download manager in Firefox. If you bookmark a website while in a Private Window, it will remain in your bookmark list.

### Myth 3: Private Browsing doesn't display any browsing history.

**Reality:** Private Browsing will, by default, [display visited sites and bookmarks as you type in the address bar](#). Firefox saves these pages during normal browsing. If you don't want to see these suggestions, you can deselect them in your Firefox Settings [Privacy & Security](#) panel under Address Bar.

#### Address Bar

When using the address bar, suggest

- ☐ Browsing history  
☐ Bookmarks  
☐ Open tabs

### Myth 4: Private Browsing will protect you from keystroke loggers and spyware.

**Reality:** Private Browsing does not protect you from malware installed on your computer. If you suspect you have malware, [take steps to remove it](#) to prevent it from happening again.

To learn more about how Firefox protects your privacy, see [Enhanced Tracking Protection in Firefox for desktop](#) and [SmartBlock for Enhanced Tracking Protection](#).

These fine people helped write this article:

[AliceWymann](#), [Michele Rodaro](#), [Joni](#), [Artist](#), [Jeff](#), [Erin S.](#), [Fabi](#), [Kalex](#), [Jeremy](#)

## Volunteer

Grow and share your expertise with others.  
Answer questions and improve our knowledge base.

[Learn More](#)

### Mozilla

[Report Trademark Abuse](#)  
[Source code](#)  
[Twitter](#)  
[Join our Community](#)  
[Explore Help Articles](#)

### Firefox

[Download](#)  
[Firefox Desktop](#)  
[Android Browser](#)  
[iOS Browser](#)  
[Focus Browser](#)

### Firefox for Developers

[Developer Edition](#)  
[Beta](#)  
[Beta for Android](#)  
[Nightly](#)  
[Nightly for Android](#)

### Firefox Accounts

[Sign In/Up](#)  
[Benefits](#)

Language

English



### Firefox Private Network

[mozilla.org](#) [Terms of Service](#) [Privacy](#) [Cookies](#) [Contact](#)

Visit Mozilla Corporation's not-for-profit parent, the Mozilla Foundation.

Portions of this content are ©1998–2022 by individual mozilla.org contributors.  
Content available under a Creative Commons license.

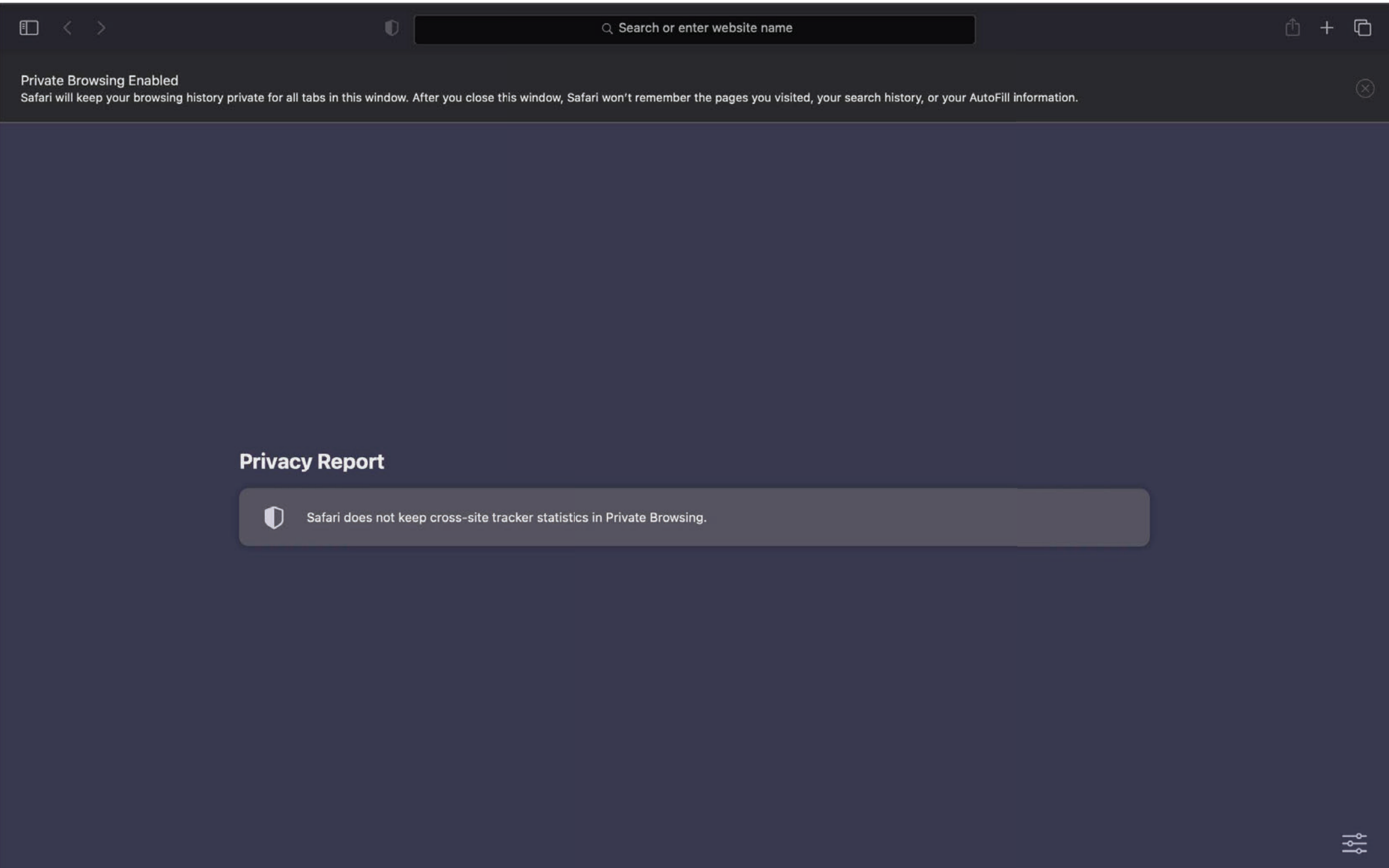
**APPENDIX L**

**SAFARI**

**PRIVATE BROWSING**

**SPLASH SCREEN**





# **APPENDIX M.1**

## **GOOGLE PRIVACY POLICY (UNHIGHLIGHTED)**



#### GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.



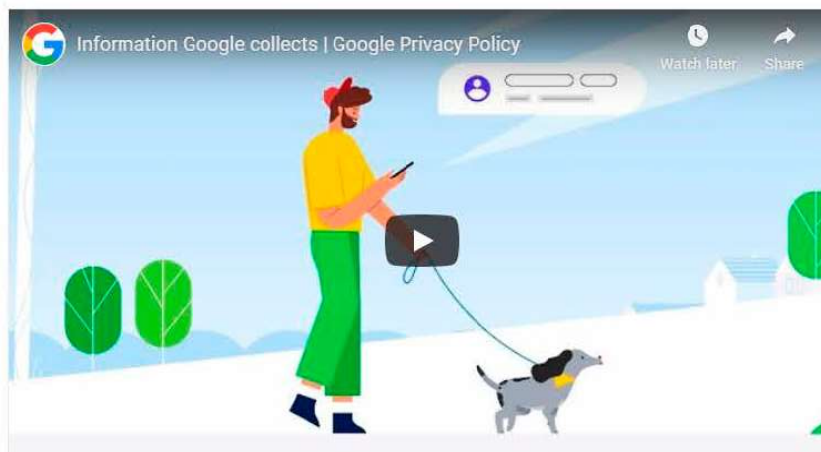


We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for [key terms](#). And if you have any questions about this Privacy Policy, you can [contact us](#).



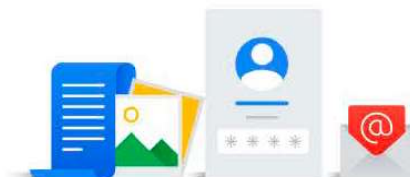
## INFORMATION GOOGLE COLLECTS

**We want you to understand the types of information we collect as you use our services**

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

**Things you create or provide to us**

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

**Information we collect as you use our services**

Your apps, browsers & devices



We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers – for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

### Your activity



We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content

- Activity on third-party sites and apps that use our services
- [Chrome browsing history you've synced with your Google Account](#)

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

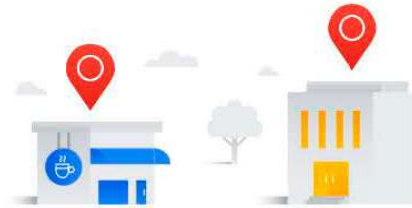
You can visit your [Google Account](#) to find and manage activity information that's saved in your account.



[Go to Google Account](#)

---

#### Your location information



We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- [IP address](#)
- [Sensor data from your device](#)
- [Information about things near your device](#), such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

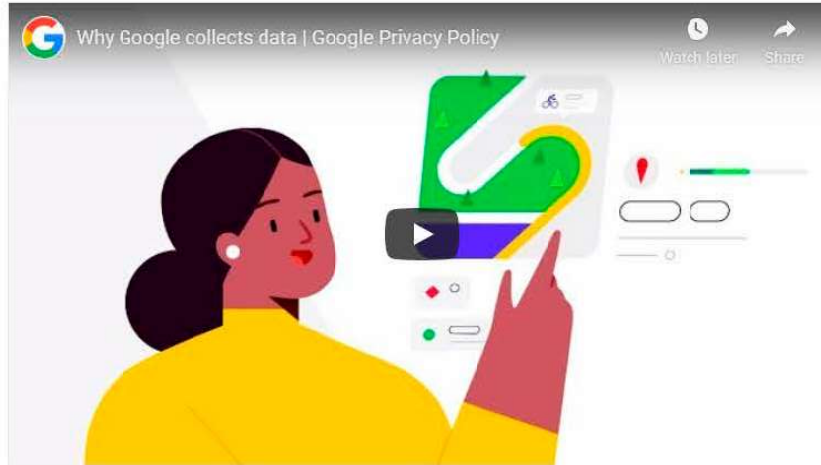
The types of location data we collect depend in part on your device and account settings. For example, you can [turn your Android device's location on or off](#) [using the device's settings app](#). You can also turn on [Location History](#) [if you want to create a private map of where you go with your signed-in devices](#).

---

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security

marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide [advertising and research services on their behalf](#).

We use various technologies to collect and store information, including [cookies](#), [pixel tags](#), local storage, such as [browser web storage](#) or [application data caches](#), databases, and [server logs](#).

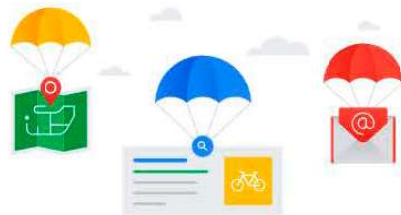


#### WHY GOOGLE COLLECTS DATA

### We use data to build better services

We use the information we collect from all our services for the following purposes:

#### Provide our services

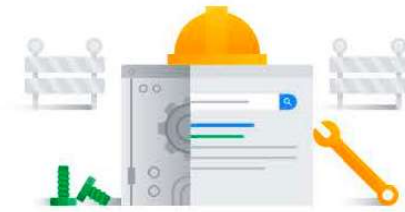


We use your information to [deliver our services](#), like processing the terms you search for in order to return results or



We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

#### Maintain & improve our services



We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

#### Develop new services



We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

#### Provide personalized services, including content and ads



We use the information we collect to customize our services for you, including providing recommendations, personalized content, and [customized search results](#). For example, [Security Checkup](#) provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you [personalized ads](#) based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on [sensitive categories](#), such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.



[Go to Ad Settings](#)

---

### Measure performance



We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer [may link information](#) about your activity from that site with activity from other sites that use our ad services.

### Communicate with you





We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

#### Protect Google, our users, and the public



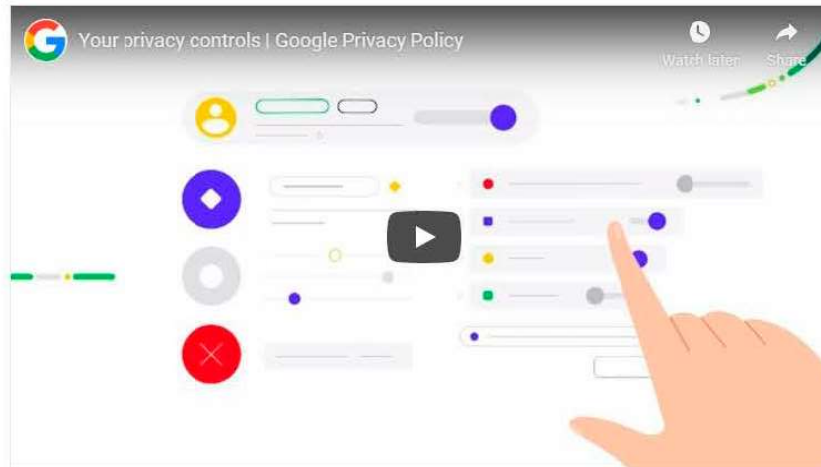
We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, [your activity on other sites and apps](#) may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.



#### YOUR PRIVACY CONTROLS

### You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the [Privacy Checkup](#), which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our [Product Privacy Guide](#).



[Go to Privacy Checkup](#)

### Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your [Google Account](#) includes:

#### Privacy controls



##### Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.

[Go to Activity Controls](#)

**Ad settings**

Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

[Go to Ad Settings](#)

**About you**

Control what others see about you across Google services.

[Go to About You](#)

**Shared endorsements**

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

[Go to Shared Endorsements](#)

**Information you share**

If you're a G Suite user, control whom you share information with through your account on Google+.

[Go to Information You Share](#)

**Ways to review & update your information****My Activity**

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

[Go to My Activity](#)

**Google Dashboard**

Google Dashboard allows you to manage information associated with specific products.

[Go to Dashboard](#)

**Your personal information**

Manage your contact information, such as your name, email, and phone number.

[Go to Personal Info](#)

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: [Choose](#) whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your [YouTube Search History](#) and your [YouTube Watch History](#).
- Ad Settings: [Manage](#) your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

## Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.



[Export your data](#)

---

You can also [request to remove content](#) from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from [specific Google services](#)
- Search for and then delete specific items from your account using [My Activity](#)
- [Delete specific Google products](#), including your information associated with those products
- [Delete your entire Google Account](#)



[Delete your information](#)

---

And finally, [Inactive Account Manager](#) allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

---

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a [cookie](#) in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services [rely on cookies to function properly](#), for things like remembering your language preferences.
- Device-level settings: Your device may have controls that determine what information we collect. For example, you can [modify location settings](#) on your Android device.



#### SHARING YOUR INFORMATION

### When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing an app in Play, your name and photo appear next to your activity. We may also display this information in [ads depending on your Shared endorsements setting](#).

### When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

#### With your consent

We'll share personal information outside of Google when we have your consent. For example, if you [use Google Home to make a reservation](#) through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We'll ask for your explicit consent to share any [sensitive personal information](#).

#### With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite), your [domain administrator](#) and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access



- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

#### For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

#### For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our [Transparency Report](#).
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to [show trends](#) about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.





## KEEPING YOUR INFORMATION SECURE

**We build security into our services to protect your information**

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like [Safe Browsing](#), Security Checkup, and [2 Step Verification](#) to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.



## EXPORTING &amp; DELETING YOUR INFORMATION

**You can export a copy of your information or delete it from your Google Account at any time**

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

[Export your data](#)

---

To delete your information, you can:

- Delete your content from [specific Google services](#)
- Search for and then delete specific items from your account using [My Activity](#)
- [Delete specific Google products](#), including your information associated with those products
- [Delete your entire Google Account](#)



[Delete your information](#)

---

#### RETAINING YOUR INFORMATION

We retain the data we collect for different periods of time depending on what it is, how we use it, and how you configure your settings:

- Some data you can delete whenever you like, such as the content you create or upload. You can also delete [activity information](#) saved in your account, or [choose to have it deleted automatically](#) after a set period of time.
- Other data is deleted or anonymized automatically after a set period of time, such as [advertising data](#) in server logs.
- We keep some data until you delete your Google Account, such as information about how often you use our services.
- And some data we retain for longer periods of time when necessary for legitimate business or legal purposes, such as security, fraud and abuse prevention, or financial record-keeping.

When you delete data, we follow a deletion process to make sure that your data is safely and completely removed from our servers or retained only in anonymized form. We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

You can read more about Google's [data retention periods](#), including how long it takes us to delete your information.



#### COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

### Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain [legal frameworks](#) relating to the transfer of data, such as the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

### California requirements

If the California Consumer Privacy Act (CCPA) applies to your information, we provide these disclosures and the [tools](#) described in this policy so you can exercise your rights to receive information about our data practices, as well as to request access to and deletion of your information. These tools allow you to review, update and delete your information, as well as export and download a copy of it. You can also [read more](#) about Google's data retention periods, and the process we follow to delete your information.

Google does not sell your personal information. We only [share your information](#) as described in this policy. Google [processes your information](#) for the purposes described in this policy, which include "business purposes" under the CCPA. These purposes include:

- **Protecting against security threats, abuse, and illegal activity.** Google uses and may disclose information to detect, prevent and respond to security incidents, and for protecting against other malicious, deceptive, fraudulent, or illegal activity. For example, to protect our services, Google may receive or disclose information about IP addresses that malicious actors have compromised.
- **Auditing and measurement.** Google uses information for analytics and measurement to understand how our services are used, as well as to fulfill obligations to our partners like publishers, advertisers, developers, or rights holders. We may disclose non-personally identifiable information publicly and with these partners, including for auditing purposes.
- **Maintaining our services.** Google uses information to ensure our services are working as intended, such as tracking outages or troubleshooting bugs and other issues that you report to us.

- **Research and development.** Google uses information to improve our services and to develop new products, features and technologies that benefit our users and the public. For example, we use publicly available information to help train Google's language models and build features like Google Translate.
- **Use of service providers.** Google shares information with service providers to perform services on our behalf, in compliance with our Privacy Policy and other appropriate confidentiality and security measures. For example, we may rely on service providers to help provide customer support.
- **Advertising.** Google processes information, including online identifiers and information about your interactions with advertisements, to provide advertising. This keeps many of our services freely available for users. You can control what information we use to show you ads by visiting your [ad settings](#).

Google also uses information to satisfy applicable laws or regulations, and discloses information in response to legal process or enforceable government requests, including to law enforcement. We provide information about the number and type of requests we receive from governments in our [Transparency Report](#).

If you have additional questions or requests related to your rights under the CCPA, [you can contact Google](#).

---

#### ABOUT THIS POLICY

### When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

### Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to [archived versions](#) for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

## RELATED PRIVACY PRACTICES

## Specific Google services

The following privacy notices provide additional information about some Google services:

- [Chrome & the Chrome Operating System](#)
- [Play Books](#)
- [Payments](#)
- [Fiber](#)
- [Google Fi](#)
- [G Suite for Education](#)
- [YouTube Kids](#)
- [Google Accounts Managed with Family Link, for Children under 13 \(or applicable age in your country\)](#)
- [Voice and Audio Collection from Children's Features on the Google Assistant](#) [↗](#)

## Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- [Your Google Account](#) [↗](#) is home to many of the settings you can use to manage your account
- [Privacy Checkup](#) [↗](#) guides you through key privacy settings for your Google Account
- [Google's safety center](#) [↗](#) helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
- [Privacy & Terms](#) provides more context regarding this Privacy Policy and our Terms of Service
- [Technologies](#) includes more information about:
  - [How Google uses cookies](#)
  - Technologies used for [Advertising](#)
  - [How Google uses pattern recognition](#) to recognize things like faces in photos
  - [How Google uses information from sites or apps that use our services](#)

## Key terms

### Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. Learn more about the [companies providing business services in the EU](#).

### Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

### Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

### Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

### Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

### Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address, and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

### IP address



Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

#### Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

#### Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

#### Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

#### Referrer URL

A Referrer URL (Uniform Resource Locator) is information transmitted to a destination webpage by a web browser, typically when you click a link to that page. The Referrer URL contains the URL of the last webpage the browser visited.

#### Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

#### Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for "cars" looks like this:

```
123.45.67.89 - 25/Mar/2008 10:15:32 -  
http://www.google.com/search?q=cars -  
Firefox 1.0.7; Windows NT 5.1 -  
740674ce2123e569
```

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.

- `25/Mar/2003 10:15:32` is the date and time of the query.
- `http://www.google.com/search?q=cars` is the requested URL, including the search query.
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used.
- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

### Unique identifiers

A unique identifier is a string of characters that can be used to uniquely identify a browser, app, or device. Different identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed.

Unique identifiers can be used for various purposes, including security and fraud detection, syncing services such as your email inbox, remembering your preferences, and providing personalized advertising. For example, unique identifiers stored in cookies help sites display content in your browser in your preferred language. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. [Learn more about how Google uses cookies.](#)

On other platforms besides browsers, unique identifiers are used to recognize a specific device or app on that device. For example, a unique identifier such as the Advertising ID is used to provide relevant advertising on Android devices, and can be [managed](#) in your device's settings. Unique identifiers may also be incorporated into a device by its manufacturer (sometimes called a universally unique ID or UUID), such as the IMEI-number of a mobile phone. For example, a device's unique identifier can be used to customize our service to your device or analyze device issues related to our services.

### ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." [Learn more about Google ads](#) and [why you may see particular ads](#).

### advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

### Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features.

### combine the information we collect



Some examples of how we combine the information we collect include:

- When you're signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. [Learn more](#)
- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. [Learn more](#)
- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based on your activity. [Learn more](#)
- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. [Learn more](#)

#### customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can [learn more here](#). You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can [search and browse privately](#) or [turn off signed-out search personalization](#).

#### deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account
- Photos and videos you upload to Google Photos are used to help you create albums, animations and other creations that you can share. [Learn more](#)
- A flight confirmation email you receive may be used to create a "check-in" button that appears in your Gmail
- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

#### detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

#### devices

For example, we can use information from your devices to help you decide which device you'd like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

#### ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

#### ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

#### Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. [Learn more](#)

#### legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our [Transparency Report](#).

#### make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it's taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

#### may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. [Learn more](#)

#### partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. [Learn more](#)

#### payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. [Learn more](#)

#### personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. [Learn more](#)

#### phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. [Learn more](#)

#### protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

#### publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate.

#### rely on cookies to function properly

For example, we use a cookie called 'lbc's' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. [Learn more](#)

#### safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or

forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.

- The "last account activity" feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. [Learn more](#)

#### sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we [require the same from advertisers that use our services](#).

#### Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

#### servers around the world

For example, we operate data centers located [around the world](#) to help keep our products continuously available for users.

#### services to make and receive calls or send and receive messages

Examples of these services include:

- Google Hangouts, for making domestic and international calls
- Google Voice, for making calls, sending text messages, and managing voicemail
- Google Fi, for a phone plan

#### show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. [Learn more](#)

#### specific Google services

For example, you can delete [your blog](#) from Blogger or a [Google Site you own](#) from Google Sites. You can also delete [reviews](#) you've left on apps, games, and other content in the Play Store.

#### specific partners



For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. [Learn more](#) about these partners and how they use your information.

### synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. [Learn more](#)

### the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you [contact most frequently](#).

### third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

### Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure [other](#) interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

### your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your [account settings](#) and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

[Learn more](#) about how Google uses data when you use our partners' sites or apps.

# **APPENDIX M.2**

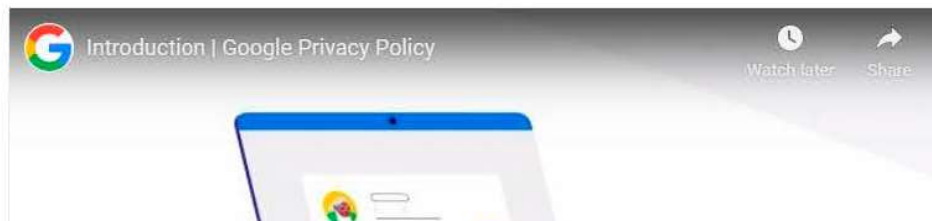
## **GOOGLE PRIVACY POLICY (HIGHLIGHTED)**



#### GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.



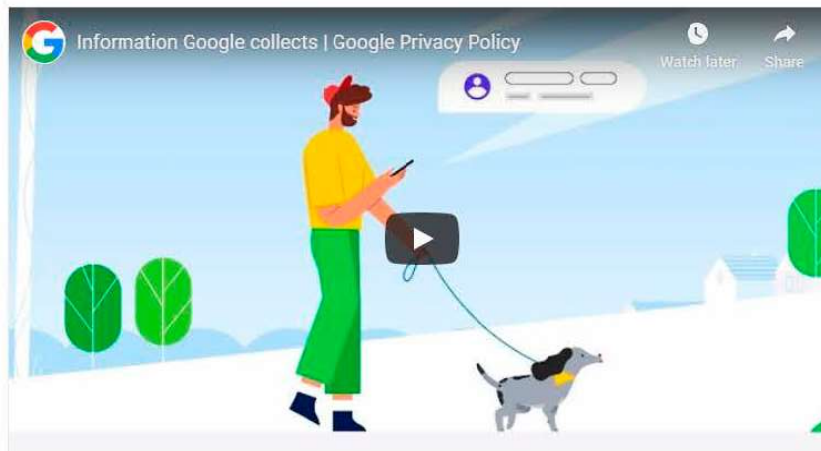


We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for [key terms](#). And if you have any questions about this Privacy Policy, you can [contact us](#).





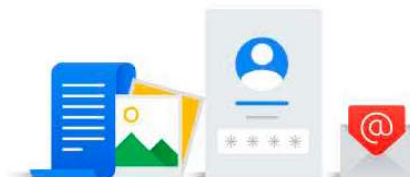
## INFORMATION GOOGLE COLLECTS

**We want you to understand the types of information we collect as you use our services**

We collect information to provide better services to all our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

**Things you create or provide to us**

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information – like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

**Information we collect as you use our services**

**Your apps, browsers & devices**



We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers – for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

#### Your activity



We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content

- [Activity on third-party sites and apps that use our services](#)
- [Chrome browsing history you've synced with your Google Account](#)

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

You can visit your [Google Account](#) to find and manage activity information that's saved in your account.



[Go to Google Account](#)

---

### Your location information



We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- [IP address](#)
- [Sensor data from your device](#)
- [Information about things near your device](#), such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

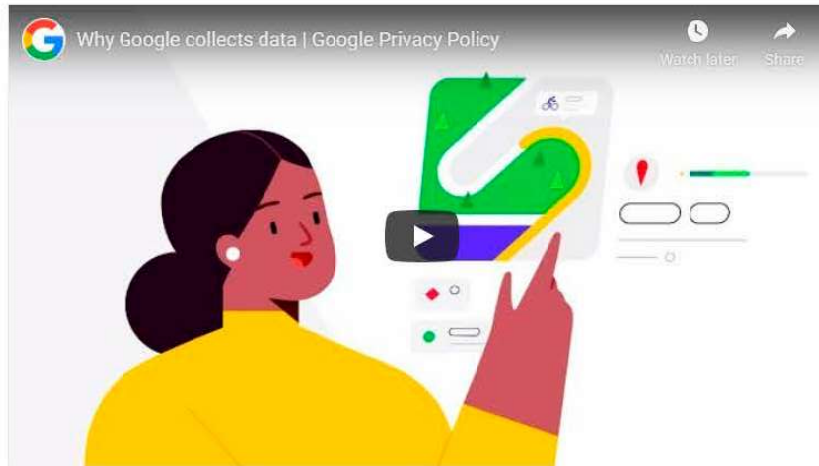
The types of location data we collect depend in part on your device and account settings. For example, you can [turn your Android device's location on or off](#) [using the device's settings app](#). You can also turn on [Location History](#) [if you want to create a private map of where you go with your signed-in devices](#).

---

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security

marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

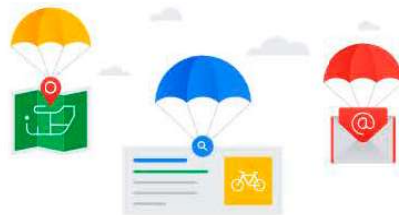


#### WHY GOOGLE COLLECTS DATA

### We use data to build better services

We use the information we collect from all our services for the following purposes:

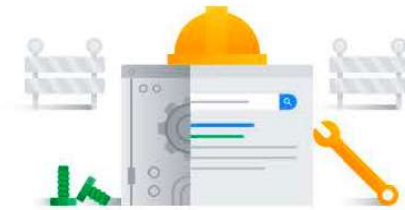
#### Provide our services



We use your information to deliver our services, like processing the terms you search for in order to return results or

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

#### Maintain & improve our services



We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

#### Develop new services



We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

#### Provide personalized services, including content and ads



We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, [Security Checkup](#) provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.



[Go to Ad Settings](#)

### Measure performance



We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.

### Communicate with you







We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

#### Protect Google, our users, and the public



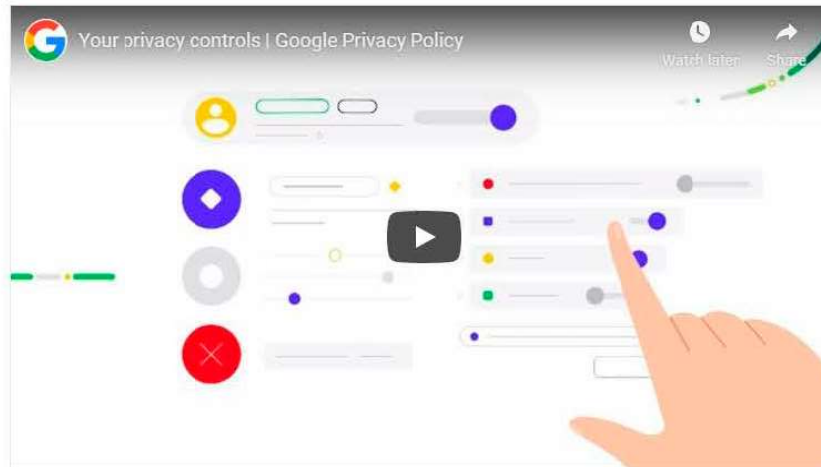
We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, [your activity on other sites and apps](#) may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.



#### YOUR PRIVACY CONTROLS

### You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the [Privacy Checkup](#), which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products – you can learn more in our [Product Privacy Guide](#).



[Go to Privacy Checkup](#)

### Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your [Google Account](#) includes:

#### Privacy controls



##### Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.

[Go to Activity Controls](#)



**Ad settings**

Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

[Go to Ad Settings](#)**About you**

Control what others see about you across Google services.

[Go to About You](#)**Shared endorsements**

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

[Go to Shared Endorsements](#)**Information you share**

If you're a G Suite user, control whom you share information with through your account on Google+.

[Go to Information You Share](#)**Ways to review & update your information****My Activity**

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

[Go to My Activity](#)**Google Dashboard**

Google Dashboard allows you to manage information associated with specific products.

[Go to Dashboard](#)**Your personal information**

Manage your contact information, such as your name, email, and phone number.

[Go to Personal Info](#)

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: Choose [whether](#) your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your [YouTube Search History](#) and your [YouTube Watch History](#).
- Ad Settings: [Manage](#) your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

## Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.



Export your data

You can also [request to remove content](#) from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from [specific Google services](#)
- Search for and then delete specific items from your account using [My Activity](#)
- [Delete specific Google products](#), including your information associated with those products
- [Delete your entire Google Account](#)



Delete your information

And finally, [Inactive Account Manager](#) allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a cookie in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services [rely on cookies to function properly](#), for things like remembering your language preferences.
- Device-level settings: Your device may have controls that determine what information we collect. For example, you can [modify location settings](#) on your Android device.



#### SHARING YOUR INFORMATION

### When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing an app in Play, your name and photo appear next to your activity. We may also display this information in [ads depending on your Shared endorsements setting](#).

### When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

#### With your consent

We'll share personal information outside of Google when we have your consent. For example, if you [use Google Home to make a reservation](#) through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We'll ask for your explicit consent to share any [sensitive personal information](#).

#### With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite), your [domain administrator](#) and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access

- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

#### For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

#### For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our [Transparency Report](#).
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to [show trends](#) about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.



## KEEPING YOUR INFORMATION SECURE

**We build security into our services to protect your information**

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like [Safe Browsing](#), Security Checkup, and [2 Step Verification](#) to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.



## EXPORTING &amp; DELETING YOUR INFORMATION

**You can export a copy of your information or delete it from your Google Account at any time**

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

[Export your data](#)

---

To delete your information, you can:

- Delete your content from [specific Google services](#)
- Search for and then delete specific items from your account using [My Activity](#)
- [Delete specific Google products](#), including your information associated with those products
- [Delete your entire Google Account](#)



[Delete your information](#)

---

#### RETAINING YOUR INFORMATION

We retain the data we collect for different periods of time depending on what it is, how we use it, and how you configure your settings:

- Some data you can delete whenever you like, such as the content you create or upload. You can also delete [activity information](#) saved in your account, or [choose to have it deleted automatically](#) after a set period of time.
- Other data is deleted or anonymized automatically after a set period of time, such as [advertising data](#) in server logs.
- We keep some data until you delete your Google Account, such as information about how often you use our services.
- And some data we retain for longer periods of time when necessary for legitimate business or legal purposes, such as security, fraud and abuse prevention, or financial record-keeping.

When you delete data, we follow a deletion process to make sure that your data is safely and completely removed from our servers or retained only in anonymized form. We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

You can read more about Google's [data retention periods](#), including how long it takes us to delete your information.





#### COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

### Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain [legal frameworks](#) relating to the transfer of data, such as the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

### California requirements

If the California Consumer Privacy Act (CCPA) applies to your information, we provide these disclosures and the [tools](#) described in this policy so you can exercise your rights to receive information about our data practices, as well as to request access to and deletion of your information. These tools allow you to review, update and delete your information, as well as export and download a copy of it. You can also [read more](#) about Google's data retention periods, and the process we follow to delete your information.

Google does not sell your personal information. We only [share your information](#) as described in this policy. Google [processes your information](#) for the purposes described in this policy, which include "business purposes" under the CCPA. These purposes include:

- **Protecting against security threats, abuse, and illegal activity.** Google uses and may disclose information to detect, prevent and respond to security incidents, and for protecting against other malicious, deceptive, fraudulent, or illegal activity. For example, to protect our services, Google may receive or disclose information about IP addresses that malicious actors have compromised.
- **Auditing and measurement.** Google uses information for analytics and measurement to understand how our services are used, as well as to fulfill obligations to our partners like publishers, advertisers, developers, or rights holders. We may disclose non-personally identifiable information publicly and with these partners, including for auditing purposes.
- **Maintaining our services.** Google uses information to ensure our services are working as intended, such as tracking outages or troubleshooting bugs and other issues that you report to us.

- **Research and development.** Google uses information to improve our services and to develop new products, features and technologies that benefit our users and the public. For example, we use publicly available information to help train Google's language models and build features like Google Translate.
- **Use of service providers.** Google shares information with service providers to perform services on our behalf, in compliance with our Privacy Policy and other appropriate confidentiality and security measures. For example, we may rely on service providers to help provide customer support.
- **Advertising.** Google processes information, including online identifiers and information about your interactions with advertisements, to provide advertising. This keeps many of our services freely available for users. You can control what information we use to show you ads by visiting your [ad settings](#).

Google also uses information to satisfy applicable laws or regulations, and discloses information in response to legal process or enforceable government requests, including to law enforcement. We provide information about the number and type of requests we receive from governments in our [Transparency Report](#).

If you have additional questions or requests related to your rights under the CCPA, [you can contact Google](#).

---

#### ABOUT THIS POLICY

### When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

### Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to [archived versions](#) for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).



## RELATED PRIVACY PRACTICES

## Specific Google services

The following privacy notices provide additional information about some Google services:

- [Chrome & the Chrome Operating System](#)
- [Play Books](#)
- [Payments](#)
- [Fiber](#)
- [Google Fi](#)
- [G Suite for Education](#)
- [YouTube Kids](#)
- [Google Accounts Managed with Family Link, for Children under 13 \(or applicable age in your country\)](#)
- [Voice and Audio Collection from Children's Features on the Google Assistant](#)

## Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- [Your Google Account](#) is home to many of the settings you can use to manage your account
- [Privacy Checkup](#) guides you through key privacy settings for your Google Account
- [Google's safety center](#) helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
- [Privacy & Terms](#) provides more context regarding this Privacy Policy and our Terms of Service
- [Technologies](#) includes more information about:
  - [How Google uses cookies](#)
  - [Technologies used for Advertising](#)
  - [How Google uses pattern recognition](#) to recognize things like faces in photos
  - [How Google uses information from sites or apps that use our services](#)

## Affiliates

### Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. Learn more about the [companies providing business services in the EU](#).

### Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

### Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

### Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

## Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.

### Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

### Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address, and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

## IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

#### Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

#### Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

#### Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

#### Referrer URL

A Referrer URL (Uniform Resource Locator) is information transmitted to a destination webpage by a web browser, typically when you click a link to that page. The Referrer URL contains the URL of the last webpage the browser visited.

#### Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

#### Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for "cars" looks like this:

```
123.45.67.89 - 25/Mar/2008 10:15:32 -  
http://www.google.com/search?q=cars -  
Firefox 1.0.7; Windows NT 5.1 -  
740674ce2123e569
```

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.

CONFIDENTIAL - SUBJECT TO PROTECTIVE ORDER

- 25/Mar/2003 10:15:32 is the date and time of the query.
- http://www.google.com/search?q=cars is the requested URL, including the search query.
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.
- 740674ce2123a969 is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

### Unique identifiers

A unique identifier is a string of characters that can be used to uniquely identify a browser, app, or device. Different identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed.

Unique identifiers can be used for various purposes, including security and fraud detection, syncing services such as your email inbox, remembering your preferences, and providing personalized advertising. For example, unique identifiers stored in cookies help sites display content in your browser in your preferred language. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. [Learn more about how Google uses cookies.](#)

On other platforms besides browsers, unique identifiers are used to recognize a specific device or app on that device. For example, a unique identifier such as the Advertising ID is used to provide relevant advertising on Android devices, and can be managed in your device's settings. Unique identifiers may also be incorporated into a device by its manufacturer (sometimes called a universally unique ID or UUID), such as the IMEI-number of a mobile phone. For example, a device's unique identifier can be used to customize our service to your device or analyze device issues related to our services.

### ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." [Learn more about Google ads and why you may see particular ads.](#)

### advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

### Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features.

### combine the information we collect



Some examples of how we combine the information we collect include:

- When you're signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. [Learn more](#)
- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. [Learn more](#)
- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based on your activity. [Learn more](#)
- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. [Learn more](#)

#### customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can [learn more here](#). You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can [search and browse privately](#) or [turn off signed-out search personalization](#).

#### deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account
- Photos and videos you upload to Google Photos are used to help you create albums, animations and other creations that you can share. [Learn more](#)
- A flight confirmation email you receive may be used to create a "check-in" button that appears in your Gmail
- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

#### detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

#### devices

For example, we can use information from your devices to help you decide which device you'd like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

#### ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

#### ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

#### Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. [Learn more](#)

#### legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our [Transparency Report](#).

#### make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it's taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

#### may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. [Learn more](#)

#### partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. [Learn more](#)

#### payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. [Learn more](#)

#### personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. [Learn more](#)

#### phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. [Learn more](#)

#### protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

#### publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate.

#### rely on cookies to function properly

For example, we use a cookie called 'lbc' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. [Learn more](#)

#### safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or

forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.

- The "last account activity" feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. [Learn more](#)

#### sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we [require the same from advertisers that use our services](#).

#### Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

#### servers around the world

For example, we operate data centers located [around the world](#) to help keep our products continuously available for users.

#### services to make and receive calls or send and receive messages

Examples of these services include:

- Google Hangouts, for making domestic and international calls
- Google Voice, for making calls, sending text messages, and managing voicemail
- Google Fi, for a phone plan

#### show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. [Learn more](#)

#### specific Google services

For example, you can delete [your blog](#) from Blogger or a [Google Site you own](#) from Google Sites. You can also delete [reviews](#) you've left on apps, games, and other content in the Play Store.

#### specific partners



For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. [Learn more](#) about these partners and how they use your information.

### synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. [Learn more](#)

### the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you [contact most frequently](#).

### third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

### Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure [other](#) interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

### your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your [account settings](#) and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

[Learn more](#) about how Google uses data when you use our partners' sites or apps.

# **APPENDIX N.1**

## **CHROME PRIVACY NOTICE (UNHIGHLIGHTED)**

# Google Chrome Privacy Notice

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read [this overview of Chrome's privacy controls](#).

## Table of contents:

- [Browser modes](#)
- [Managing users in Chrome](#)
- [Safe Browsing practices](#)
- [Privacy practices of using apps, extensions, themes, services, and other add-ons](#)
- [More information](#)

---

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

## Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the [network actions prediction](#) feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.
- [Cookies](#) or data from websites that you visit.
- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can [delete your browsing history information](#).
- You can manage or delete stored browsing data from the [Cookies and Site Data dialog](#).
- You can stop Chrome from [accepting cookies](#). [Learn more](#).
- You can review stored passwords in Chrome settings. [Learn more](#).
- You can view and manage your stored Autofill information. [Learn more](#).

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your [Google Account](#) by turning on sync, or, in the case of payment cards and billing information, choosing specific payment card and billing information to store in your Google Payments account. [Learn More](#).

## How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive [standard log information](#), including your system's IP address and data from [cookies](#). In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google or the website you visited to help determine the extent of the attack and how the attack functions. Google provides participating website owners with reports about attacks occurring on their sites.

**Prerendering.** To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. [Learn more](#).



**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, Chrome automatically shares your location with your default search engine if the Chrome app has permission to access your location and you haven't blocked geolocation for the associated web site. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active users.

**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the omnibox or the search box on the new tab page in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the omnibox or the search box on the new tab page in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing in the omnibox or in the search box on the new tab page, and what other people are searching for. [Learn more](#). Predictions can also be based on your browsing history. [Learn more](#).

**Navigation assistance.** When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

**Autofill and password management.** In order to improve Chrome's Autofill and password management services, Chrome sends Google limited, anonymous information about the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more](#).

**Payments.** When you are signed into Chrome with your Google account, Chrome may offer to save payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you have cards saved locally in Chrome, Chrome may prompt you to save them to your Google Payments account. If you use a payment card from your Google Payments account or choose to save your payment card in your Google Payments account for future use, Chrome will collect information about your computer and share it with Google Pay to protect you from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls](#).

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more](#).

**Usage statistics and crash reports.** By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. In general, usage statistics do not include web page URLs or personal information, but, if you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. If you have enabled Chrome sync, Chrome may combine any declared age and gender information from your Google account with our statistics to help us build products better suited for all demographics. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We may share aggregated, non-personally identifiable information publicly and with partners — like publishers, advertisers or web developers. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more](#).

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

## Identifiers in Chrome

Chrome includes a number of unique and non-unique identifiers necessary to power features and functional services. For example, if you use push messaging, an identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more](#).
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more](#).

## Sign-in and Sync Chrome modes

You also have the option to use the Chrome browser while signed in to your Google Account, with or without sync enabled.



**Sign in on Desktop.** On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. You can turn this off in settings. [Learn more](#). If you are signed in to your Google Account on desktop, Chrome may offer to save your payment cards and related billing information to your Google Payments account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it on the [Data from Chrome sync Dashboard](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required and sync cannot be disabled because it provides parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable synchronization of most data types. [Learn More](#). The [Privacy Notice for Google Accounts created in Family Link](#) applies to Chrome sync data stored in those accounts.

### How Chrome handles your synced information

When you enable sync with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more](#).

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more](#).

## Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- Basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

### How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.

**Browser configuration changes.** When you make changes to your browser configuration, like bookmarking a web page or changing your settings, this

information is saved. These changes are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

**Profile information.** In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

---

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. [Learn more.](#)

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device.

---

## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

### How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive [standard log information](#), including an IP address and [cookies](#).

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. [Learn more.](#)

The following Safe Browsing features are specific to Chrome:



- If you have turned on Safe Browsing's Enhanced Protection mode, Chrome provides additional protections, and sends Google additional data, as described in Chrome settings. [Learn more](#). Some of these protections may also be available as standalone features, subject to separate controls, where Standard Protection is enabled.
- If you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google" and Safe Browsing is enabled, Chrome sends Google the full URL of each site you visit to determine whether that site is safe. If you also sync your browsing history without a sync passphrase, these URLs will be temporarily associated with your Google account to provide more personalized protection. This feature is disabled in incognito and guest modes.
- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.
- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, or if you are signed in to your Google Account and choose to notify Google, Chrome will also flag your Google Account as likely phished.
- If you are signed in to your Google Account, Chrome will also warn you when you use a username and password that may have been exposed in a data breach. To check, when you sign in to a site, Chrome sends Google a partial hash of your username and other encrypted information about your password, and Google returns a list of possible matches from known breaches. Chrome uses this list to determine whether your username and password were exposed. Google does not learn your username or password, or whether they were exposed, as part of this process. This feature can be disabled in Chrome settings. [Learn more](#).
- On desktop and Android versions of Chrome, you can always choose to [disable the Safe Browsing feature within Chrome settings](#). On iOS versions of Chrome, Apple controls the Safe Browsing technology used by your device and may send data to Safe Browsing providers other than Google.

---

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

### Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

## Server Log Privacy Information

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:

123.45.67.89 - 25/Mar/2003 10:15:32 - https://www.google.com/search?q=cars - Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;
- https://www.google.com/search?q=cars is the requested URL, including the search query.;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123e969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID assigned to their device the user the next time they/s/he visits Google from that particular computer).

---

## More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.

Google complies with certain [legal frameworks](#) relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Framework. [Learn more](#).

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

### Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

Follow us



#### Chrome Family

Other Platforms

Chromebooks

Chromecast

Chrome Cleanup Tool

#### Enterprise

Download Chrome Browser

Chrome Browser for Enterprise

Chrome Devices

Chrome OS

Google Cloud

G Suite

#### Education

Google Chrome Browser

Devices

Web Store

#### Dev and Partners

Chromium

Chrome OS

Chrome Web Store

Chrome Experiments

Chrome Beta

Chrome Dev

Chrome Canary

#### Stay Connected

Google Chrome Blog

Chrome Help

Google

[Privacy and Terms](#)

[About Google](#)

[Google Products](#)



Help

English - United States

[Learn more](#)

Ok, Got it

# **APPENDIX N.2**

## **CHROME PRIVACY NOTICE (HIGHLIGHTED)**



# Google Chrome Privacy Notice

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read [this overview of Chrome's privacy controls](#).

## Table of contents:

- [Browser modes](#)
- [Managing users in Chrome](#)
- [Safe Browsing practices](#)
- [Privacy practices of using apps, extensions, themes, services, and other add-ons](#)
- [More information](#)

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

## Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the [network actions prediction](#) feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.
- [Cookies](#) or data from websites that you visit.
- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can [delete your browsing history information](#).
- You can manage or delete stored browsing data from the [Cookies and Site Data dialog](#).
- You can stop Chrome from [accepting cookies](#). [Learn more](#).
- You can review stored passwords in Chrome settings. [Learn more](#).
- You can view and manage your stored Autofill information. [Learn more](#).

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your [Google Account](#) by turning on sync, or, in the case of payment cards and billing information, choosing specific payment card and billing information to store in your Google Payments account. [Learn More](#).

## How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive [standard log information](#), including your system's IP address and data from [cookies](#). In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google or the website you visited to help determine the extent of the attack and how the attack functions. Google provides participating website owners with reports about attacks occurring on their sites.

**Prerendering.** To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. [Learn more](#).

**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, Chrome automatically shares your location with your default search engine if the Chrome app has permission to access your location and you haven't blocked geolocation for the associated web site. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active users.

**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the omnibox or the search box on the new tab page in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the omnibox or the search box on the new tab page in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing in the omnibox or in the search box on the new tab page, and what other people are searching for. [Learn more](#). Predictions can also be based on your browsing history. [Learn more](#).

**Navigation assistance.** When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

**Autofill and password management.** In order to improve Chrome's Autofill and password management services, Chrome sends Google limited, anonymous information about the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more](#).

**Payments.** When you are signed into Chrome with your Google account, Chrome may offer to save payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you have cards saved locally in Chrome, Chrome may prompt you to save them to your Google Payments account. If you use a payment card from your Google Payments account or choose to save your payment card in your Google Payments account for future use, Chrome will collect information about your computer and share it with Google Pay to protect you from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls](#).

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more](#).



**Usage statistics and crash reports.** By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. In general, usage statistics do not include web page URLs or personal information, but, if you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. If you have enabled Chrome sync, Chrome may combine any declared age and gender information from your Google account with our statistics to help us build products better suited for all demographics. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We may share aggregated, non-personally identifiable information publicly and with partners — like publishers, advertisers or web developers. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more](#).

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

## Identifiers in Chrome

Chrome includes a number of unique and non-unique identifiers necessary to power features and functional services. For example, if you use push messaging, an identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more](#).
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more](#).

## Sign-in and Sync Chrome modes

You also have the option to use the Chrome browser while signed in to your Google Account, with or without sync enabled.



**Sign in on Desktop.** On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. You can turn this off in settings. [Learn more](#). If you are signed in to your Google Account on desktop, Chrome may offer to save your payment cards and related billing information to your Google Payments account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it on the [Data from Chrome sync Dashboard](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required and sync cannot be disabled because it provides parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable synchronization of most data types. [Learn More](#). The [Privacy Notice for Google Accounts created in Family Link](#) applies to Chrome sync data stored in those accounts.

### How Chrome handles your synced information

When you enable sync with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more](#).

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more](#).

## Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode](#) or [guest mode](#). In these modes, Chrome won't store certain information, such as:

- Basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

### How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.

**Browser configuration changes.** When you make changes to your browser configuration, like bookmarking a web page or changing your settings, this

information is saved. These changes are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

**Profile information.** In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

---

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. [Learn more.](#)

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device.

---

## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

### How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive [standard log information](#), including an IP address and [cookies](#).

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. [Learn more.](#)

The following Safe Browsing features are specific to Chrome:



- If you have turned on Safe Browsing's Enhanced Protection mode, Chrome provides additional protections, and sends Google additional data, as described in Chrome settings. [Learn more](#). Some of these protections may also be available as standalone features, subject to separate controls, where Standard Protection is enabled.
- If you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google" and Safe Browsing is enabled, Chrome sends Google the full URL of each site you visit to determine whether that site is safe. If you also sync your browsing history without a sync passphrase, these URLs will be temporarily associated with your Google account to provide more personalized protection. This feature is disabled in incognito and guest modes.
- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.
- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, or if you are signed in to your Google Account and choose to notify Google, Chrome will also flag your Google Account as likely phished.
- If you are signed in to your Google Account, Chrome will also warn you when you use a username and password that may have been exposed in a data breach. To check, when you sign in to a site, Chrome sends Google a partial hash of your username and other encrypted information about your password, and Google returns a list of possible matches from known breaches. Chrome uses this list to determine whether your username and password were exposed. Google does not learn your username or password, or whether they were exposed, as part of this process. This feature can be disabled in Chrome settings. [Learn more](#).
- On desktop and Android versions of Chrome, you can always choose to [disable the Safe Browsing feature within Chrome settings](#). On iOS versions of Chrome, Apple controls the Safe Browsing technology used by your device and may send data to Safe Browsing providers other than Google.

---

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

### Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

## Server Log Privacy Information

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:

123.45.67.89 - 25/Mar/2003 10:15:32 - https://www.google.com/search?q=cars - Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;
- https://www.google.com/search?q=cars is the requested URL, including the search query.;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123e969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID assigned to their device the user the next time they/s/he visits Google from that particular computer).

---

## More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.

Google complies with certain [legal frameworks](#) relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Framework. [Learn more](#).

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

### Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

Follow us   

#### Chrome Family

Other Platforms

Chromebooks

Chromecast

Chrome Cleanup Tool

#### Enterprise

Download Chrome Browser

Chrome Browser for Enterprise

Chrome Devices

Chrome OS

Google Cloud

G Suite

#### Education

Google Chrome Browser

Devices

Web Store

#### Dev and Partners

Chromium

Chrome OS

Chrome Web Store

Chrome Experiments

Chrome Beta

Chrome Dev

Chrome Canary

#### Stay Connected

Google Chrome Blog

Chrome Help

Google

[Privacy and Terms](#)

[About Google](#)

[Google Products](#)

 [Help](#)

[English - United States](#)

[Learn more](#) 

Ok, Got it

# **APPENDIX O**

# **NEW ACCOUNT CREATION**

# **AGREEMENT**





## Privacy and Terms

To create a Google Account, you'll need to agree to the [Terms of Service](#) below.

In addition, when you create an account, we process your information as described in our [Privacy Policy](#), including these key points:

### Data we process when you use Google

- When you set up a Google Account, we store information you give us like your name, email address, and telephone number.
- When you use Google services to do things like write a message in Gmail or comment on a YouTube video, we store the information you create.
- When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity – including information like the video you watched, device IDs, IP addresses, cookie data, and location.
- We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.

### Why we process it

We process this data for the purposes described in [our policy](#), including to:

- Help our services deliver more useful, customized content such as more relevant search results;
- Improve the quality of our services and develop new ones;
- Deliver personalized ads, depending on your account settings, both on Google services and on sites and apps that partner with Google;
- Improve security by protecting against fraud and abuse; and
- Conduct analytics and measurement to understand how our services are used. We also



You're in control of the data we collect & how it's used

have partners that measure how our services are used. [Learn more](#) about these specific advertising and measurement partners.

## Combining data

We also combine this data among our services and across your devices for these purposes. For example, depending on your account settings, we show you ads based on information about your interests, which we can derive from your use of Search and YouTube, and we use data from trillions of search queries to build spell-correction models that we use across all of our services.

## You're in control

Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data now by clicking "More Options" below. You can always adjust your controls later or withdraw your consent for the future by visiting My Account ([myaccount.google.com](https://myaccount.google.com)).

### More options ^

Customize your Google experience by confirming your personalization settings and the data stored with your account.

You can always learn more about these options, adjust them, and review your activity in your Google Account ([account.google.com](https://account.google.com)).



## Web & App Activity

Saves your activity on Google sites and apps, including searches and associated info like location. Also saves activity from sites, apps, and devices that use Google services, including Chrome history. This helps Google provide better search results, suggestions, and personalization across Google services. Activity older than 18 months will be automatically deleted. You can change your auto-delete option, stop saving activity, or delete it manually at [account.google.com](https://account.google.com).



Save my Web & App Activity in my Google Account



☐ Don't save my Web & App Activity in my Google Account

---

[Learn more about Web & App Activity](#)

☐ **Ad personalization**

Google can show you ads based on your activity on Google services (such as Search or YouTube), and on websites and apps that partner with Google.

☒ Show me personalized ads

☐ Show me ads that aren't personalized

---

[Learn more about Ad personalization](#)

☐ **YouTube History**

Saves the YouTube videos you watch and the things you search for on YouTube. This helps Google give you better recommendations, remember where you left off, and more. Activity older than 36 months will be automatically deleted. You can change your auto-delete option, stop saving activity, or delete it manually at [account.google.com](https://account.google.com).

☒ Save my YouTube History in my Google Account

☐ Don't save my YouTube History in my Google Account

---

These settings apply wherever you are signed in to your new Google Account.

☐ Send me occasional reminders about these settings

[Cancel](#)

[I agree](#)

**APPENDIX P**  
**CONSENT BUMP**  
**AGREEMENT**  
**AND FAQ PAGE**

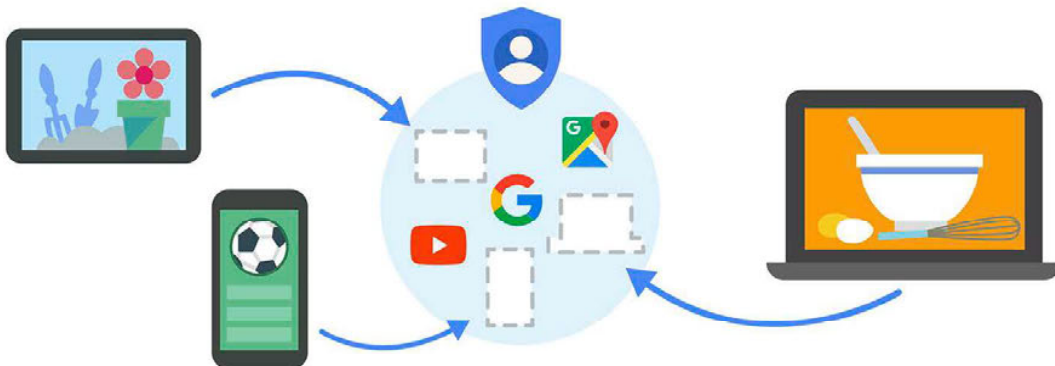


## Some new features for your Google Account

We've introduced some optional features for your account, giving you more control over the data Google collects and how it's used, while allowing Google to show you more relevant ads.

What changes if you turn on these new features?

1. More information will be available in your *Google Account*, making it easier for you to review and control



When you use Google services like Search and YouTube, you generate data – things like what you've searched for and videos you've watched. You can find and control that data in *My Account* under the **Web & App Activity** setting.

With this change, this setting may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.

2. Google will use this information to make ads across the web more relevant for you



In *My Account*, the **Ads Personalization** setting currently lets Google use data in your account to tailor ads that appear in Google products.

With this change, this setting will also let Google use data in your account to improve the relevance of ads on websites and apps that partner with Google.

These settings apply across all of your signed-in devices and across all Google services. You can change them any time in *My Account*. [Learn more](#) about these features, including how they affect shared devices.

## What's still the same?

- Google does not sell your personal information to anyone
- You control the types of information we collect and use at *My Account* ([myaccount.google.com](https://myaccount.google.com))

**Choose I AGREE to turn these features on or MORE OPTIONS for more choices.**

---

[MORE OPTIONS](#)

[I AGREE](#)

---

## More about these new features

We think these new features will make your Google experience better and we hope this page will help you decide what's right for you. Read on for more about the change and how it affects the data Google collects, your privacy settings, and the ads you see.



## Why does Google collect data and where does it come from?

Data helps us make our services faster, smarter, and more useful for you. For example, when you allow Google Maps to know your location, it can show you the quickest way home.

Some of the data that Google collects comes from our own products and some of it comes from your visits to sites and apps that [partner with Google](#). These new features allow you to make more of this information visible in your *Google Account*, so your info is easier to review and control. The new features also expand our ability to make Google services better, including making the ads you see in Google products and across the web more relevant to you.

## How does Google give you control over your information?

We created *MyAccount* ([myaccount.google.com](https://myaccount.google.com)) to give you one central place where you can quickly access and manage your information. You also have easy-to-use settings there that allow you to decide how you want our services to work for you.

These new features introduce updates to two key privacy settings in your account:

- Your **Web & App Activity** setting lets you see and control data you generate when using Google services, like things you search for and search results you select. Google uses this data to improve your experience, including giving you better search results. If you turn on these new features, your *Web & App Activity* may also include browsing data from Chrome and activity from sites and apps that [partner with Google](#), including those that show ads from Google.
- Your **Ads Personalization** setting lets Google use data from your account, such as the searches you've done and your location, to make the ads we show you more relevant and useful. If you turn on these new features, Google can use that same data to improve the relevance of ads on sites and apps that partner with Google and across your signed-in devices.

If you decide not to turn on these new features, your settings and Google experience will stay the same.

## What if you use more than one *Google Account* at the same time?

You can control your settings separately for each of your accounts. But if you use more than one account at the same time, Google applies the settings from your default account.

On the web, your default account is the first account you use each time you sign in to a new browser. On mobile devices, the default account depends on your operating system and the apps you use.

For example, if you sign in on the web with two different Google accounts, Google will use

For example, if you sign in on the web with two different Google accounts, Google will use *Web & App Activity* and *Ads Personalization* settings from the account you signed in to first, both to save data and to personalize your experience.

---

## Why do ads matter and how does Google decide what ads to show?

Ads allow Google to offer Gmail, You Tube, Search, Maps, and many other services for free. When you use those services, our goal is to make the ads there as relevant for you as possible. The information in your *Google Account* helps us do that.

Ads also allow other sites and apps to offer their content for free. More than 2 million of them, likely many that you use, rely on Google to provide the ads they show. This change now makes it possible for us to use the same information in your *Google Account* to improve the ads we show you while you're signed in and visiting those sites and apps.

In more technical terms, instead of personalizing ads using a cookie ID for each of your devices, as we do today, this change makes it possible to use a single identifier associated with your account that gets used in Google products and across the web.

While we try to show you the best ads possible, we know we don't always get it right, and that's why you have ways to control the ads you see. For example, *Mute This Ad* lets you remove ads you don't find relevant. And with this change, your ads preferences work whenever you're signed in – across all Google products and on all your signed-in devices.

---

## What do we mean by “websites and apps that partner with Google”?

Many websites and apps use Google technologies to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like partners who use Google Analytics to improve the ads they show).

As you use these sites, your web browser may send certain information to Google that may include the web address of the page that you're visiting, your IP address, or cookies previously set by the site or Google. In the case of mobile apps, this could also include the name of the app and an identifier that helps us to determine which ads we've served to other apps on your device.

The features described today don't change the types of data collected from these websites and apps – they simply change how that data is stored and used.

---

See the [Google Privacy Policy](#) for more information about what data we collect, why we collect it, and what we do with it.

---

# **EXHIBIT 79**

## **5/20/22 EXPERT REPORT OF MARK KEEGAN**

**Redacted Version of  
Document Sought to  
be Sealed**





**KEEGAN & DONATO**  
CONSULTING, LLC

31 Purchase Street, Ste. 3-4  
Rye, New York 10580  
914.967.9421  
www.keegandonato.com

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

<hr/>		)	
		)	
Chasom Brown, et al.,		)	
		)	
Plaintiffs,		)	
		)	
v.		)	Civil Action No.: 5:20-cv-03664-YGR
		)	
Google LLC,		)	
		)	
Defendant.		)	
<hr/>		)	

**Expert Report of Mark Keegan:**  
**Rebuttal of Expert Report of Professor On Amir**

**Keegan & Donato Consulting, LLC**  
**May 20, 2022**



**KEEGAN & DONATO**  
CONSULTING, LLC

31 Purchase Street, Ste. 3-4  
Rye, New York 10580  
914.967.9421  
www.keegandonato.com

## Table of Contents

I. Executive Summary of Opinions .....	1
II. Summary of Assignment .....	3
III. Firm Overview .....	4
IV. Analysis of the Amir Studies.....	6
Global deficiencies and limitations of the Amir Studies.....	7
Poor data quality.....	8
Tainted respondents – lawsuit awareness.....	12
Tainted respondents – recent survey takers.....	13
Incorrect survey universe.....	14
Irrelevant and incomplete browser use.....	16
Summary – Global limitations.....	18
Consumer Perceptions and Expectations Study.....	19
Inappropriate reading test .....	19
Failure to replicate the market.....	23
Irrelevant variables – unclear entities .....	25
Irrelevant variables – oversimplification of data types .....	26
Summary – Consumer Perceptions and Expectations Study .....	28
Interpretation Study .....	28
Failure to replicate the market.....	28
Leading questions.....	31
Irrelevant variables – oversimplification of data types .....	33
Inappropriate reading test .....	33
Summary – Interpretation Study.....	34
Likelihood of Use Study .....	35
Flawed disclosure modifications.....	35
Failure to account for confounding variables .....	39
Self-serving “Learn More” exposure .....	40
Summary – Likelihood of Use Study.....	41
Conclusions – Amir Report .....	42



**KEEGAN & DONATO  
CONSULTING, LLC**

31 Purchase Street, Ste. 3-4  
Rye, New York 10580  
914.967.9421  
[www.keegandonato.com](http://www.keegandonato.com)

V. The Keegan Study .....	42
Summary of assignment .....	42
Methodology .....	44
Study integrity .....	44
Study objectives .....	44
Study population .....	45
Study design .....	45
Data collection .....	46
Sampling .....	47
Bias management .....	47
Questionnaire .....	49
Sample characteristics .....	56
Findings .....	57
VI. Analysis of Google Internal Documents .....	59
VII. Conclusions .....	62

**Exhibits**

- Exhibit 1—Mark Keegan C.V.
- Exhibit 2—Documents Considered
- Exhibit 3—Amir Studies—Open-Ended Coding
- Exhibit 4—Keegan Study—Questionnaire
- Exhibit 5—Keegan Study—Tabulated Data
- Exhibit 6—Keegan Study—Untabulated Data
- Exhibit 7—Keegan Study—Disposition of Contacts
- Exhibit 8—Summary of Google Internal Documents



**KEEGAN & DONATO**  
CONSULTING, LLC

31 Purchase Street, Ste. 3-4  
Rye, New York 10580  
914.967.9421  
www.keegandonato.com

## **I. Executive Summary of Opinions**

1. Pursuant to the Court's Standing Order,<sup>1</sup> this section includes an executive summary of each opinion that I will offer regarding the April 15, 2022 Expert Report of Professor On Amir (the "Amir Report") and related topics.
2. Opinion 1: As described in Section IV, all three of the studies presented in the Amir Report (the "Amir Studies") suffer from material methodological and analytical deficiencies and limitations which render the findings presented in the Amir Report an unreliable and invalid basis for drawing opinions and conclusions regarding Class Members' perceptions, expectations, and behaviors with regard to Google's private browsing mode ("PBM") data collection practices. Those deficiencies and limitations include:
  - a. Poor data quality;
  - b. Tainted respondents;
  - c. An incorrect survey universe;
  - d. Incorrect and incomplete browser usage questions.
3. Opinion 2: As described in Section IV, Professor Amir's Consumer Perceptions and Expectations Study provides no valid or reliable evidence regarding the perceptions and expectations of any reasonable Class Member or any proportion of either of the two Classes and therefore provides no support for Professor Amir's stated opinions with respect to any Class Members.

---

<sup>1</sup> [https://cand.uscourts.gov/wp-content/uploads/judges/gonzalez-rogers-ygr/Judge-Gonzalez-Rogers\\_-Standing-Order-In-Civil-Cases.pdf](https://cand.uscourts.gov/wp-content/uploads/judges/gonzalez-rogers-ygr/Judge-Gonzalez-Rogers_-Standing-Order-In-Civil-Cases.pdf)

4. Opinion 3: As described in Section IV, Professor Amir's Interpretation Study provides no valid or reliable evidence regarding how any reasonable Class Member or any proportion of either of the two Classes would interpret Google's PBM disclosures in a real-world scenario and therefore provides no support for Professor Amir's stated opinions with respect to any Class Members.
5. Opinion 4: As described in Section IV, Professor Amir's Likelihood of Use Study provides no valid or reliable evidence regarding the extent to which, if at all, any reasonable Class Member or any proportion of either of the two Classes would continue using Chrome Incognito for private browsing if adequately informed about Google's PBM data collection and storage practices and therefore provides no support for Professor Amir's stated opinions with respect to any Class Members.
6. Opinion 5: As described in Section V, as a rebuttal to the Amir Studies, I designed and conducted a consumer study of 1,052 respondents (the "Keegan Study") that addressed deficiencies and limitations of the Amir Studies and also provides a reliable set of findings regarding the reasonable beliefs of Class Members during the Class Period, with common proof that can be broken down into the two separate Classes and provides quantitative results reflecting what a reasonable consumer would have understood.
7. Opinion 6: As described in Section V, based on the Keegan Study results, it is clear both that a reasonable member of each of the two Classes and also virtually all Class Members would not have understood or believed that they had consented to Google's collection and storage of their private browsing data.
8. Opinion 7: As described in Section V, the Keegan Study results show that **93.1 percent** of respondents were misinformed about Google's PBM data collection and storage practices:

<i>Base: All respondents (n=1,052)</i>	<b>% Respondents</b>
<b><i>Misinformed about Google PBM data collection and storage practices</i></b>	
Google does not collect and save my Internet browsing activity in private browsing mode	54.8
I have not given consent to Google to collect and save my Internet browsing activity when I browse the Internet in PBM	20.2
I have given consent to Google to collect and save my Internet browsing activity in PBM only when visiting a Google website	11.8
I have given consent to Google to collect and save my Internet browsing activity in PBM only when signed in to my Google account	3.6
Indicated a belief that Google would not collect and save at least one type of data displayed in the matrix table	2.8
<b>Total misinformed about Google PBM data collection and storage practices</b>	<b>93.1</b>
<b><i>Informed or don't know</i></b>	<b>6.9</b>
<b>Total</b>	<b>100.0</b>

9. Opinion 8: As described in Section VI, I also considered documents produced by Google that relate to the relevant issues addressed in the Amir Studies and the Keegan Study. Those Google documents are fundamentally inconsistent with and undermine Professor Amir's findings and opinions, and they are in turn consistent with and provide support for my findings and opinions.

## II. Summary of Assignment

10. For the purposes of this rebuttal report, I was asked to review and opine on an expert report submitted by Google's expert, Professor On Amir (the "Amir Report"). The Amir Report presents the findings of three consumer research studies (the "Amir Studies"), which are discussed in detail below.
11. In light of the material deficiencies and limitations of the Amir Studies, as discussed in this report, I also was asked to design and execute a methodologically-sound consumer research study to reliably gauge consumer beliefs with regard to Google's collection and storage of PBM data (the "Keegan Study").

12. I was also asked to review and consider the documents produced by Google in this litigation, to assess the extent to which those were consistent with the findings and opinions of Professor Amir and my own findings and opinions.
13. My analysis of the Amir Studies, a full detailing of the objectives, methodology, findings, and conclusions of the Keegan Study, and my assessment of the Google-produced documents are presented in this report.

### **III. Firm Overview**

14. I am a principal at Keegan & Donato Consulting, a consulting firm serving litigators and their clients. Our areas of expertise include marketing analysis, intellectual property, consumer survey research, damages analysis, forensic economic analysis, and related disciplines.
15. Keegan & Donato Consulting designs and executes methodologically sound consumer survey research studies and conducts objective evaluation of existing survey research as well as collaborates on a wide range of marketing and complex commercial litigation issues. We are also regularly engaged by clients for non-litigation consulting assignments related to marketing research and strategy.
16. Over the course of my career, I have personally conducted over 1,000 consumer surveys reaching more than 250,000 consumers. Many of these surveys have been admitted into evidence in federal courts, state courts, at arbitration, to the Trademark Trial and Appeal Board, the National Advertising Division of the Council of Better Business Bureaus, and the United States International Trade Commission.
17. In the past four years, I have been deposed or testified at trial in conjunction with my involvement in litigation matters 31 times. I have also served as a rebuttal witness.
18. I am a graduate of the University of Georgia's *Principles of Market Research Program*. This comprehensive course of study, developed in concert with the Market Research Institute International (MRII), is a post-graduate program for marketing industry professionals covering all aspects of the market research process. Coursework is based on the MRII's Market Research Core Body of Knowledge (MRCBOK), a compilation of the underlying principles and essential skills that comprise the market research process. Certification is conferred only upon participants who demonstrate mastery of concepts presented in 284



detailed module studies across 13 core areas of market research, as determined via rigorous proctored examinations. The University of Georgia's *Principles of Market Research Program* is endorsed by all major market research and insights industry associations, including ESOMAR and the Insights Association.

19. My educational background additionally includes a J.D. from Brooklyn Law School and a B.A. in History from Pace University. I have completed coursework in the MBA program at the Lubin School of Business at Pace University and in Harvard University's Corporate Finance Certificate program. I have also served as a Registered Representative, National Association of Securities Dealers (Series 7, expired).
20. I have spent the entirety of my career in marketing-related roles. I have served as a marketing consultant to private clients and have advised on a wide range of issues including product development and rollout, advertising, consumer feedback and intelligence, the product life-cycle, and other issues concerning marketing and marketing research. Over the past two decades, I have founded and successfully operated two marketing consulting and marketing research firms, Keegan & Company LLC and Keegan & Donato Consulting, LLC. Prior to that, I served in various marketing management and research roles in both large and small companies including Information Markets Corp., Affiliation Networks, Inc., Uptick Technologies, Cosmos Internet Solutions, Fact Set Research Systems, and BMW of North America, Inc.
21. As a marketing expert, I have formulated winning brand positioning strategies for some of the best-known consumer brands and services. While at Keegan & Company, I worked with General Electric to position its consumer credit services as an industry leading advantage available to all. In my time with Information Markets, I worked with consumer brands such as Nike, Pepsi, and Subaru to deliver online engagement services to a younger audience. I also collaborated with AOL, Excite, and NBC to develop and launch an online forum to exchange ideas and expertise among category thought leaders.
22. I am a member of the American Marketing Association (AMA), the preeminent professional association for marketing practitioners and scholars. From the AMA I have earned the designation of Professional Certified Marketer (PCM). The AMA confers the PCM certification upon individuals who have demonstrated a mastery of comprehensive and core marketing knowledge and principles. PCM certification requires rigorous testing, ongoing

professional development, and a commitment to upholding the highest standards in the marketing field. The AMA only accepts into the PCM certification program applicants with demonstrated professional experience in the field of marketing.

23. Keegan & Donato Consulting is a member of ESOMAR, the leading global association for market, social, and opinion research, the American Association for Public Opinion Research (AAPOR), a professional organization of more than 2,000 public opinion and survey research professionals in the United States and from around the world, the International Trademark Association (INTA), and the Association for Consumer Research (ACR). I have published in an ESOMAR compendium on the benefits of methodologically sound marketing research. I have taught CLE-accredited courses on survey research for litigation at the Florida Bar's Annual IP Symposium and have addressed the Pennsylvania Bar Association's Intellectual Property Law group with a presentation on the building blocks of survey research for litigation, consumer research best practices, and current trends in the industry.
24. Additional information about my credentials is provided at Exhibit 1 to this report. Exhibit 1 also lists the matters in which I have provided testimony over the last four years.
25. Prior to this engagement, I had personally used some of the private browsing modes discussed in this report (including Chrome Incognito mode), but I did not know that Google receives and saves information from my private browsing mode activities, including in particular when I am visiting non-Google websites without being signed in to any Google account. This was something I first learned when I become engaged as an expert for this litigation.

#### **IV. Analysis of the Amir Studies**

26. The Amir Studies purport to "evaluate consumer understanding, perceptions, and expectations specific to the facts of this case, and to evaluate whether and to what extent consumers' understanding, perceptions, and expectations affect their likelihood of using a specific internet browser or browser feature."<sup>2</sup> The Amir Report describes these studies as follows:

---

<sup>2</sup> Amir Report, ¶ 2.

- The **Consumer Perceptions and Expectations Study**, which Professor Amir states was intended “to assess whether and to what extent users expect different types of entities to receive or to not receive data (such as IP address, URLs of the sites users visit, and cookies) when they visit websites while in private browsing mode”;<sup>3</sup>
- The **Interpretation Study**, which Professor Amir states was intended “to assess whether and to what extent users expect Google to receive or to not receive URLs of the sites users visit, IP addresses, and cookies placed on users’ browsers during their Incognito session after reviewing the Incognito Splash Screen and ‘Learn More’ page” as well as other Google disclosures;<sup>4</sup> and
- The **Likelihood of Use Study**, which Professor Amir states was intended “to assess whether and to what extent modification of certain language on the Incognito Splash Screen and the ‘Learn More’ page that address Plaintiffs’ criticisms of those documents...impacts users’ likelihood of using Chrome in Incognito mode for private browsing.”<sup>5</sup>

27. All three of the Amir Studies suffer from material methodological and analytical limitations which call into question the reliability and validity of the findings and opinions that are presented in the Amir Report. Whereas some of these limitations are global and apply to all of the Amir Studies, other limitations are specific to the individual study methodologies. I will discuss the deficiencies and limitations of the Amir Studies in the Sections that follow.

#### **Global deficiencies and limitations of the Amir Studies**

28. The three studies presented in the Amir Report collectively suffer from a number of methodological and analytical deficiencies and limitations which undermine their usefulness as valid and reliable evidence on the issues that are relevant to this matter. Those deficiencies and limitations in turn significantly impact the reliability of the opinions and conclusions drawn from the resulting study data.

---

<sup>3</sup> Amir Report, ¶ 3.

<sup>4</sup> Amir Report, ¶ 8.

<sup>5</sup> Amir Report, ¶ 13.

***Poor data quality***

29. All of the Amir Studies suffer from data quality issues. This is evidenced by the low-quality verbatim responses to the open-ended format question<sup>6</sup> used in the Amir Studies. Toward the end of each questionnaire, all three Amir Studies asked respondents the following question: “Prior to this survey, were you or were you not aware of any lawsuits related to private browsing mode?”<sup>7</sup> Respondents who indicated that they were aware of at a lawsuit related to private browsing mode were asked a follow-up question wherein they were asked to “describe the lawsuit” in their own words in a text box.<sup>8</sup>
30. When employing open-ended questions in a survey, the researcher typically will engage in a data cleansing process whereby low-quality and nonsense responses are identified and flagged for removal from the final data set. This is an important step in the data analysis process because respondents who do not engage with the survey questionnaire in the intended manner—i.e., those who appear to not take the survey seriously, those who provide low-effort responses, gibberish, etc.—are of questionable reliability. The process of removing low-quality and other problematic responses from the data set reinforces the integrity of the data and ensures that external biases, including respondent disengagement, keyboard mashing, copy/paste responses, guesses, bot activity, flippant responses, and other respondents who provide undesirable and untruthful data are not included in the survey results.
31. A review of the open-ended responses to the Amir Studies shows that problematic responses were not identified and removed from the studies even though the study data maps<sup>9</sup> included the coding structure to remove low-quality responses.<sup>10</sup> Indeed, low-quality responses are

---

<sup>6</sup> An open-ended question is a question that requires respondents to answer in their own words. In an online survey, open-ended questions typically provide respondents with a text box wherein they can type their verbatim response.

<sup>7</sup> Amir Report Appendices, pp. F.1-14, F.2-19, F.3-10.

<sup>8</sup> A “Don’t know / Unsure” option was provided. See Amir Report Appendices, pp. F.1-14, F.2-19, F.3-10.

<sup>9</sup> A data map is a listing of the data fields and corresponding numeric values that are represented in a database.

<sup>10</sup> The data maps for all three Amir Studies contain coding categories for “Verbatim Check Failed” and “Quality Check Failed.” See Consumer Perceptions and Expectations Study data file, 2203704.xlsx, Interpretation Study data file, 2203487.xlsx, Likelihood of Use Study data file, 2203523.xlsx.

pervasive across all three of the Amir Studies. Table 1 below provides examples of a few of the many low-quality responses from the Consumer Perceptions and Expectations Study:

*Table 1. Exemplar low-quality verbatim responses, Consumer Perceptions and Expectations Study*

<b>Response ID</b>	<b>“Describe the lawsuit...” (verbatim response)</b>
kxdm40p9nerpzuf	dfddfgdgdggdgg
w4fxv8uv2xg9afjv	Everything very good and very nice 🤩
5an1aemb8u0yn0sx	good, nice, cool, better, fun, easy
b6bfb0am1r5r4z1u	I WAS VISITING A PORN SITE
kw9x1m5bq39eftxu	Is very good
qbk92qzu7x8fvrkv	Yes I’m going to get my hair done today and I just got home from work and I just got home from work and I just got home from work and I
h3mghcp7s62wsn54	very good value
jf6enycp89wupkw9	OVERALL ITS A VERY HELPFULL
xy351ak03myuzrnm	My lawsuit regarging is the best idea in this option
kqme1qr4tqqr3w97	IT IS VERY LOVELY

32. Similarly, the Interpretation Study contains many low-quality responses. Table 2 below provides a sampling of the many low-quality responses from the Interpretation Study:

Table 2. Exemplar low-quality verbatim responses, Interpretation Study

Response ID	"Describe the lawsuit..." (verbatim response)
8316y92sewfqn8yw	afsdafsfdsf.dasf ads gfdsf sagdfgwdsaf ew.df af to long.
y9xs861jzd1b6dq4	ALL IS AMAZING
5k3rqgdnkbf0fb40	Best concept and very interested
d0ys8m6jbn3yr5am	dfsdfsdfsdf sdfsdffsdf sfsdfsdf sdf sdfsdf
vtcbm89wzsq7g7av	Excellent and wonderful great unique different from other products very reliable and trustworthy
ef60amndkk7a5w0n	excellent mode, I like very much
3bfrtjc2qbchkef5	F GD FGDFGDF GDFGDFD
xh3asbjd3c2hez50	Hedjk and night in the next day and ktexjk in the world at all of the index finger and I think I can get the first place
bjputkttrsvbr08g	Hey buddy I just got home from raider I love you mama bye mama
f53us0vk1nc14t98	very fantastic excellent

33. The Likelihood of Use Study was also materially impacted; Table 3 below provides exemplar low-quality verbatim responses from the Likelihood of Use Study:

*Table 3. Exemplar low-quality verbatim responses, Likelihood of Use Study*

<b>Response ID</b>	<b>“Describe the lawsuit...” (verbatim response)</b>
53eavqse4mjtgnsp	all is very perfect and very nice
evbgm6t5c446awdy	nm u hug sara kmne ki kaj
0rzaq2bzxb4mc6ct	Nnnnnnnnn
g574ejn318qac9va	EXCELLENT THE BEST
z3vb7fd9aqacac82	Fggddffcvvxxxxccccccffgggggggggggh hhhhhhhhhhhh
yftp4gwnywdh6dvd	I LOVE THIS
72bdh6jetu6q35wz	I love you too hot to handle Netflix cast and crew of the series
5e5yuwc8na2q8dft	I hope so fatboy I’m so excited
bpe62kt8qebmc0e8	is design and model is excellent for the customer is interesting
nfm5991h8kq5nchs	please I was in my heart is broken heart and soul and friends and family

34. The examples shown above are representative of a systemic deficiency in the Amir Studies’ data. Across all three Amir Studies, 217 of 555 open-ended responses provided by respondents on this question—39.1 percent—should have been categorized as low-quality<sup>11</sup> and removed from the data sets. Because not all respondents provided open-ended responses, it is reasonable to extrapolate this analysis to the overall samples used in the Amir Studies to conclude that approximately 40 percent of all respondents who participated in the Amir Studies may have been low-quality respondents.
35. The inclusion of data from respondents who clearly were not taking the study seriously compromises the integrity of all three Amir Studies. Because the Amir Studies are based on a

---

<sup>11</sup> 2203704.xlsx, 2203487.xlsx, 2203523.xlsx.



foundation of a significant number of low-quality respondents, Professor Amir's opinions and conclusions are not reliable or supported and should be considered with caution.

***Tainted respondents – lawsuit awareness***

36. In addition to low-quality responses, all three Amir Studies included respondents who had an awareness of the current litigation. Table 4 below provides a sampling of the verbatim responses provided by such respondents.

*Table 4. Exemplar respondents aware of current litigation*

<b>Response ID</b>	<b>Study</b>	<b>“Describe the lawsuit...” (verbatim response)</b>
9wpguy78djwbj1ux	Cons. Percep/ Expectations	Brown vs. Google LLC
6c5yyq9mp8n0b7xf	Cons. Percep/ Expectations	Claims against Google using information obtained in private browsing
kgefj5zbh314pbmc	Cons. Percep/ Expectations	Google selling private information
p5ku4bq6pezhx0em	Cons. Percep/ Expectations	Google spying through google analytics
9aa7w9h815mz325z	Cons. Percep/ Expectations	I don't know much about it but it was a lawsuit that revealed that Google collects data from incognito and ever since I dint trust them as much.
e7tzjmvh1k01mfqc	Cons. Percep/ Expectations	I remember hearing someone sued Google over thinking incognito mode was 100% private or something like that.
9um6tz1kboxatfpsb	Cons. Percep/ Expectations	I was aware of the google chrome private browser mode lawsuit. Supposedly that google chrome's private browsing mode wasn't so private.
2ce91bzgm2ww18ne	Interpretation	2020 google faced a demand of 5m \$ for information tracked in incognito mode
t7g7zmf7hhkhd8v5	Interpretation	Chrome will not store the browsing history, Cookies and sites data
uvzb08syppad8bry	Interpretation	Google being face with lawsuit over tracking their users in private mode
12mbemw8sx1unnrb	Interpretation	Google had a lawsuit against them for tracking in incognito mode
49ghc7w1jjwd6a8k	Interpretation	Google still gathering information from incognito

wpjzpe0uhxj30fdv	Interpretation	Google still might see what you're doing even if you using private wen
vyk3enr1u269udsu	Likelihood of Use	Google accidentally giving out info pertaining to it's users of incognito mode
ah0nwp98x8q639xg	Likelihood of Use	Google is ordered to face a \$5 billion lawsuit alleging Chrome's Incognito browsing mode collects users' web history.
3a7nqcf88ds4byr9	Likelihood of Use	Google still track user's browsing data in private mode.
74c9szdc9cqfv5hc	Likelihood of Use	Google supposedly shared private information that it said it would protect.
r24aes5712g1vnn1	Likelihood of Use	I am aware of a lawsuit against google alleging that they still collect user data even in incognito mode
85ukh7gmte8mdbxx	Likelihood of Use	I read that there is a lawsuit against Google incognito browsing because some information is still tracked and the statement on Google's incognito page is insufficient
pk82crzc7bahnazy	Likelihood of Use	I'm not sure if the details about who was suing Google, but the lawsuit was about the incognito mode not blocking all of the sensitive data that by design it promises too.
uhce24wzm1te8n3z	Likelihood of Use	That Google was being sued for tracking peoples data while they were supposedly in incognito mode.

37. In all, 25.3 percent of all respondents across all three Amir Studies indicated an awareness of a lawsuit related to private browsing mode, and as shown in the Table 4 above, many provided open-end responses that appear to specifically identify this litigation. None of these respondents were removed from the study data based on this criterion.<sup>12</sup> Again, as with the low-quality responses cited above, this is surprising considering the study data maps included the coding structure to remove such low-quality responses.<sup>13</sup>

#### ***Tainted respondents – recent survey takers***

38. It is also notable that a material proportion of respondents across all three Amir Studies indicated that they had recently taken another survey related to private browsing. In each of

<sup>12</sup> 2203704.xlsx, 2203487.xlsx, 2203523.xlsx.

<sup>13</sup> 2203704.xlsx, 2203487.xlsx, 2203523.xlsx.

the three Amir Studies, respondents were asked, “In the past three months, have you or have you not taken any other survey related to private browsing mode?”<sup>14</sup> Across the three studies, a total of 13.7 percent of participants indicated that they had taken a survey related to private browsing mode in the past three months.<sup>15</sup> Despite the fact that information regarding recent survey activity was solicited, none of these respondents were removed from the Amir Studies.

***Incorrect survey universe***

39. Properly defining the population from which a survey samples—the study’s “universe,” i.e., those whose perceptions are relevant to the issue(s) being studied—is of vital importance to the reliability and validity of the study. When conducting a survey, “selection of the proper universe is a crucial step, for even if the proper questions are asked in a proper manner, if the wrong persons are asked, the results are likely to be irrelevant.”<sup>16</sup>
40. The proper universe for a consumer survey or surveys presented in a class action matter should include representative members of the proposed class or classes. In this case, the classes are defined in the Third Amended Complaint<sup>17</sup> as follows:
  - Class 1 – All Chrome browser users with a Google account who accessed a non-Google website containing Google tracking or advertising code using such a browser and who were (a) in “Incognito mode” on that browser and (b) were not logged into their Google account on that browser, but whose communications, including identifying information and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present (the “Class Period”).
  - Class 2 – All non-Chrome browser users with a Google account who accessed a non-Google website containing Google tracking or advertising code using any such browser and who were (a) in “private browsing mode” on that browser, and (b) were not logged into their Google account on that browser, but whose communications, including identifying information and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present (the “Class Period”).

---

<sup>14</sup> Amir Report Appendices, pp. F.1-15, F.2-20, F.3-11.

<sup>15</sup> Consumer Perceptions and Expectations Study, 18.1 percent; Interpretation Study, 10.1 percent; Likelihood of Use Study, 15.0 percent. See Consumer Perceptions and Expectations Study data file, 2203704.xlsx, Interpretation Study data file, 2203487.xlsx, Likelihood of Use Study data file, 2203523.xlsx.

<sup>16</sup> McCarthy, J.T. (2020). *McCarthy on Trademarks and Unfair Competition*, 5th Ed., §32:159.

<sup>17</sup> Third Amended Complaint, ¶ 192.

41. As noted above, the Class Period in this matter spans the period back to June 1, 2016. Anyone with a Google account who used one of the private browsing modes at issue during the Class Period is a potential member of the class and should have been eligible for participation in the Amir Studies.
42. The Amir Studies did not target all potential Class Members, but instead screened respondents only on private browsing mode use in the past six months. Potential respondents were asked:<sup>18</sup>

In the past six months, which of the following features, if any, have you used on your internet browser(s)?  
(Select all that apply)

☐ Customized home page

☐ Bookmarks

☐ Screenshot tool

☐ Dark mode for visual display

☐ Private browsing mode

☐ Website translator

☐ Other (Please specify)

☐ Don't know / Unsure

Continue

43. The Amir Studies' screening questions employed a time window which excluded more than 90 percent of the Class Period, and only captured usage after the lawsuit was filed. The Amir Studies did not seek, and the resulting data does not reflect, the beliefs and expectations of respondents who used PBM more than six months prior to the execution of the Amir Studies, despite the fact that such respondents are relevant to the current litigation. In short, the beliefs, expectations, and behaviors of potential Class Members who used PBM between the start of the Class Period and the start of data collection for the Amir Studies—a period spanning approximately 4.5 years—is not known and cannot be determined from the Amir Studies' data.

<sup>18</sup> Amir Report Appendices, pp. G.1-9, G.2-9, G.3-9.

44. Because Professor Amir employed an inappropriate survey universe consisting only of a small fraction of potential Class Members, the Amir Studies' participants are not representative of the broader population of potential Class Members. As such, the findings presented in the Amir Report cannot be considered a valid and reliable source of information with respect to the relevant issues in this matter and Professor Amir's opinions and conclusions based on this data are unsupported and unreliable. This inappropriate universe is something that I addressed and corrected in the Keegan Study.

***Irrelevant and incomplete browser use***

45. The screening criteria for all three Amir Studies required respondents to indicate which Internet browsers they currently use. Respondents were presented with a list of eight browsers<sup>19</sup> along with an "Other" option. Respondents were permitted to, and often did, select multiple browsers.
46. After identifying the browser(s) they had used, respondents were asked about their PBM usage. Respondents were asked, "In the past six months, which of the following features, if any, have you used on your internet browser(s)? (Select all that apply),"<sup>20</sup> where an option for "Private browsing mode" was provided, among other features.
47. Importantly, participants were not asked about the browser(s) upon which they use PBM; rather, the Amir Studies ascertain only that respondents use certain browsers and use PBM on at least one of those browsers. Indeed, for most respondents, it remains unknown which browser(s) they used for PBM browsing.
48. It is my understanding that the scope of this case is limited to private browsing in Chrome, Safari, and/or Edge/Internet Explorer.<sup>21</sup> Therefore, a respondent that does not use private browsing in one of those three Internet browsers is not part of the defined Classes in this case and should not be included in the Amir Studies' universe. Nevertheless, a review of the data

---

<sup>19</sup> Additionally, a fabricated browser ("Odeon") was included for screening purposes. See, for example, Amir Report Appendices, p. F.1-4.

<sup>20</sup> Amir Report Appendices, pp. F.1-5, F.2-5 F.3-5.

<sup>21</sup> It is my understanding from counsel that the scope of this case is limited to private browsing in Chrome, Safari, and/or Edge/Internet Explorer.

across the three Amir Studies shows that 6.2 percent of participants did not, in fact, use Chrome, Safari, or Edge/Internet Explorer at all, but rather used some other browser.<sup>22</sup>

49. An additional 41.1 percent of participants selected Chrome, Safari, and/or Edge/Internet Explorer and at least one of the other five browsers listed.<sup>23</sup> By indicating that they used a combination of relevant browsers and irrelevant browsers (for the purpose of this litigation), and because of the flawed question design asking simply if they used private browsing on some (unknown) browser, it cannot be determined whether this 41.4 percent of the sample are actually Class Members. Over 41 percent of the Amir Studies' respondents therefore may fall outside the defined Classes in this matter.
50. An example illustrates the problem with Professor Amir's approach. In the Consumer Perceptions and Expectations Study, the respondent with ID record 222 indicated that he/she had used Chrome, Firefox, *and* Opera.<sup>24</sup> Whereas the study does establish that this respondent engaged in private browsing generally, it is unclear—and indeed, unknowable—from the study data whether he/she engaged in private browsing in Chrome. It is entirely possible that this respondent exclusively performed private browsing in Firefox and/or Opera—i.e., irrelevant browsers. To the extent this is true, this respondent is not a Class Member but was included in Professor Amir's Consumer Perceptions and Expectations Study. This problem affects all three of the Amir Studies.
51. In sum, reviewing the Amir Studies' data shows that 6.2 percent of the sample did not use any of the Internet browsers at issue in this lawsuit and should therefore have been excluded from the universe. An additional 41.4 percent of the sample are potentially non-Class Members, although one cannot know for certain given the limitations of the study design. Accordingly, 47.6 percent of respondents—nearly half the study universe—are either certainly not Class Members or potentially not Class Members. This is a material limitation of the Amir Studies which undermines the findings and opinions in the Amir Report. This is something that I addressed and corrected in the Keegan Study.

---

<sup>22</sup> 2203704.xlsx, 2203487.xlsx, 2203523.xlsx.

<sup>23</sup> The other browsers were Brave, Mozilla Firefox, Opera, DuckDuckGo, and Other. 2203704.xlsx, 2203487.xlsx, 2203523.xlsx.

<sup>24</sup> 2203704.xlsx, uuid: wxuqedgjkzh958sz.

***Summary – Global limitations***

52. The inclusion of low-quality respondents and tainted respondents compromises the overall integrity of the Amir Studies. Across all three Amir Studies, approximately 40 percent of respondents appear to be of unacceptably low quality with respect to their engagement with the study. Although such respondents introduce biases into the study data, and the Amir Studies included the mechanics to identify and remove such respondents in the data coding schema, this data cleansing exercise was never performed.
53. Additionally, 30 percent of respondents indicated that they were aware of a lawsuit involving private browsing mode or were recent survey participants on the subject.<sup>25</sup> Although these questions were included in each study and, again, the mechanics to remove those respondents was built into the data coding schema, these respondents were not removed, thereby rendering nearly one-third of respondents included in the Amir Report of dubious quality by the studies' own measurement.
54. The Amir Studies also used an incorrect survey universe which screened respondents only on private browsing mode use in the past six months. The Amir Studies' screening questions employed a time window which excluded more than 90 percent of the Class Period. As such the resulting data does excludes Class Members who used PBM more than six months prior to the execution of the Amir Studies, resulting in a flawed survey universe.
55. Finally, the Amir Studies included respondents who only used irrelevant Internet browsers and/or PBMs and are not part of the defined Classes. Indeed, 47.6 percent of respondents—nearly half the study universe—are either certainly not Class Members or potentially not Class Members based on their browser usage. Inclusion of these problematic respondents further erodes the reliability and applicability of the studies' data.
56. For these reasons, I do not consider the opinions and conclusions presented in the Amir Report (which are based on the Amir Studies' flawed and unreliable data) to be reliable evidence on the relevant issues in this matter.

---

<sup>25</sup> 2203704.xlsx, 2203487.xlsx, 2203523.xlsx.



### **Consumer Perceptions and Expectations Study**

57. The Consumer Perceptions and Expectations Study was purportedly intended “to assess whether and to what extent users expect different types of entities to receive or to not receive data (such as IP address, URLs of the sites users visit, and cookies) when they visit websites while in private browsing mode.”<sup>26</sup> In addition to the deficiencies and limitations identified above, the following sections discuss additional deficiencies and limitations of this study.<sup>27</sup>

#### ***Inappropriate reading test***

58. The Consumer Perceptions and Expectations Study fails to collect objective information regarding respondents’ perceptions and expectations because it forces respondents to study various disclosures and formulate their answers based on those forced exposures. In all cases, the study design made the survey stimuli available for respondents to reference when answering the key questions of interest.
59. As noted by litigation research commentator Dr. Jacob Jacoby, “after exposing respondents to a...stimulus, the researcher has two basic options: either remove the stimulus from view before asking the critical substantive questions, those designed to shed light on the legal issues being tested, or leave it in full view of the respondent while asking these questions.”<sup>28</sup> A design wherein the stimulus remains in the respondent’s view has sometimes been referred to as a “reading test,” because respondents have an opportunity to study, or “read,” the stimulus when answering key questions of interest.
60. In this case, the Consumer Perceptions and Expectations Study made available images of various disclosures while respondents answered the key measurement questions.
61. One of the reasons that researchers commonly remove stimuli from the view of the respondent when administering key study measures is that leaving the stimuli in sight creates

---

<sup>26</sup> Amir Report, ¶ 3.

<sup>27</sup> It is my understanding based on information from Plaintiffs’ Counsel that Plaintiffs are not asserting any claims based on Firefox private browsing. To the extent that the Amir Studies present data related to Firefox browsing, those calculations are irrelevant to my analysis. Additionally, I understand that Plaintiffs are asserting claims based on Edge/Internet Explorer private browsing. The Amir Studies did not include analyses of Edge/Internet Explorer private browsing and as such, Professor Amir does not offer any opinions on Edge/Internet Explorer.

<sup>28</sup> Jacoby, J. (2013). *Trademark Surveys, Volume 1: Designing, Implementing, and Evaluating Surveys*, p. 566.

an elevated risk of response bias. Rather than serving as an objective measure of what the respondent believes about the relevant issue, this methodological design risks being overly suggestive. By making the stimuli available, the design tends to suggest to the respondent that information they glean from studying the stimulus is a suitable answer regardless of their personal opinions or beliefs. This risk has been referred to as a “reading test,” wherein the respondent simply reads back what is in front of them and their actual understanding and beliefs as to the issue being studied are not measured.<sup>29</sup>

62. To mitigate the potential for response bias when using visual stimuli, researchers commonly remove such stimuli from view prior to administering the key measures of the study. Doing so forces the respondent to consider their individual interpretation of the stimuli to which he or she was previously exposed, thereby more closely approximating marketplace conditions. When a consumer evaluates a product or service in the marketplace—e.g., uses a private browsing mode in an Internet browser—they do not have a researcher asking them about their beliefs about the product or service as they are looking at it. Thus, it does not make sense to create this scenario in the survey environment.
63. By exposing the consumer to the stimulus, then removing it, *and then* asking about their beliefs and opinions as to the key research issues, the researcher is able to access the consumer’s actual real-world marketplace beliefs and understanding, not the more artificial and contrived response created when the interviewer allows the respondent to study the stimulus while answering the question.
64. Removing the stimulus from view prior to asking the consumer about their beliefs is especially important when it is the defendant’s expert that is conducting the study. When a defendant’s messaging or behavior has been accused of being inaccurate or misleading, it becomes essential that the research professional investigate that claim in the most objective way possible to avoid the appearance of introducing bias, or in any way “padding” the results in favor of his or her client. The burden on the research professional to minimize every opportunity for bias is critical to maintaining the integrity of the study data, as surveys are too easily and subtly manipulated to affect a desired outcome.

---

<sup>29</sup> Swann, J.B. (2005). “A ‘Reading’ Test Or A ‘Memory’ Test: Which Survey Methodology Is Correct?” *The Trademark Reporter*, Vol. 95, p. 876-877.

65. Expanding on this issue, Jacoby observes:

In situations where defendant's goods or advertising is allegedly likely to cause confusion, deception, or to mislead, it seems obvious that *defendant's* survey should not ask questions of respondents while the stimulus remains in front of the respondent. If there was a propensity for the respondent to be confused or deceived, guided by the questions being asked, they could review the stimulus for information that pertains to the question, and, in this way, disabuse themselves of any confusion or deception they might otherwise have experienced.<sup>30</sup> [Emphasis in original.]

66. In this case, the Consumer Perceptions and Expectations Study forced respondents to review Google's disclosures and made the study stimuli available to respondents throughout the administration of the key study measures. The potential benefit here is to the Defendant, Google, as the study design purports to measure expectations as to the types of information consumers expect entities to receive when they are in PBM. To the extent that respondents study and glean information from the stimuli in front of them (i.e., engage in the reading test), this creates the illusion that respondents are more informed about Google's PBM data collection and storage practices than they may actually be. Such respondents are potentially influenced by the survey instrument itself and may not be representative of the broader population of potential Class Members that would not be subject to such influences.
67. The deficiency of the reading test scenario is compounded by the format of the questions asked, which are constructed to be of a factual nature and do not ask about the users' beliefs. For example, in the first key measure, respondents are presented with the following:

---

<sup>30</sup> Jacoby, J. (2013). *Trademark Surveys, Volume 1: Designing, Implementing, and Evaluating Surveys*, p. 573.

76%

(The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.)

While in Incognito mode, do the companies that own the websites you visited during the session receive or not receive the data from your Incognito session (such as IP address, URLs of the sites you visit, and cookies)?

Please base your answer on the screens you reviewed.  
(Select a point on the scale. If you do not have enough information, please select "I don't feel I have enough information to answer this question")

Companies that own the websites I visited during the session do receive the data from my Incognito session



Companies that own the websites I visited during the session probably receive the data from my Incognito session

It is uncertain whether companies that own the websites I visited during the session receive the data from my Incognito session

Companies that own the websites I visited during the session probably do not receive the data from my Incognito session

Companies that own the websites I visited during the session do not receive the data from my Incognito session

☐ I don't feel I have enough information to answer this question

Continue

68. This question presents respondents with a factual proposition: “While in Incognito mode, do the companies that own the websites you visited during the session receive or not receive the data from your Incognito session (such as IP address, URLs of the sites you visit, and cookies)?”<sup>31</sup> Rather than using opinion-based language (“*do you believe* that...” or which “best reflects *your understanding*...” or “best reflects *your beliefs* ...”), the Consumer Perceptions and Expectations Study question format utilizes an inappropriate quiz-like format (“*do* the companies...”) to suggest that the answer is present in the disclosures that the respondent considered and has available for review. This limitation is compounded by the

<sup>31</sup> Amir Report Appendices, p. F.1-11.

fact that respondents are instructed to “base your answer on the screens you reviewed” and that those screens are available for further study on the same page as the question. This is not an objective measurement of respondents’ perceptions and expectations regarding Google’s PBM data collection and storage practices.

69. The “open book” reading test format does not measure consumer perceptions and expectations regarding Google’s PBM data collection and storage practices, but rather invites respondents to search for and find the “correct” answers to the questions within the curated materials provided. Because it makes use of an unreliable and biased reading test methodology, the findings of the Consumer Perceptions and Expectations Study (in contrast to the Keegan Study, described below) should be viewed as nothing more than a test of the respondent’s ability to read from a webpage. Those findings provide no reliable or useful information regarding the perceptions and expectations of any Class Members and no support for Professor Amir’s stated opinions regarding Class Members.

***Failure to replicate the market***

70. The negative implications of the reading test format of the Consumer Perceptions and Expectations Study are exacerbated by the fact that the study design also fails to accurately replicate a realistic marketplace scenario. It is important when designing a study intended to measure consumer perceptions about a product or service to recreate—to the extent possible within the artificial survey environment—a user experience within the questionnaire which faithfully and accurately replicates the experience the respondent would have in the real world.<sup>32</sup> Indeed, “while the survey setting is necessarily artificial, the survey expert must make every reasonable effort to duplicate the marketplace conditions under which consumers are likely to encounter the [product or service] at issue.”<sup>33</sup> This is the standard to which the researcher must strive if the research is to be considered a valid measure of consumer perceptions about the relevant issue, and the standard I applied for the Keegan Study.

---

<sup>32</sup> Morales, A. C., Amir, O., & Lee, L. (2017). “Keeping It Real in Experimental Research—Understanding When, Where, and How to Enhance Realism and Measure Consumer Behavior.” *Journal of Consumer Research*, Vol. 44, p. 465-476.

<sup>33</sup> Edwards, G. K., (2012). “The Daubert Revolution and Lanham Act Surveys.” in *Trademark and Deceptive Advertising Surveys*, Diamond & Swann (eds.), p. 346.

71. In this case, the Consumer Perceptions and Expectations Study does not accurately recreate the experience that consumers have when using Chrome and Safari in PBM (and also omits Edge/Internet Explorer and includes irrelevant findings regarding Firefox—see “Irrelevant and incomplete browser use” section above). Specifically, the Consumer Perceptions and Expectations Study forces respondents into an unrealistic scenario whereby they are forced to review disclosures in ways that are inconsistent with actual user behaviors.
72. Using the Chrome browser as an example, the first stimulus exposure in this study was to the Incognito splash screen. Respondents were forced to view the Incognito splash screen for 30 seconds before being allowed to continue to the next screen.<sup>34</sup> Next, respondents were forced to view a Chrome help screen that the questionnaire asserts would display when the “Learn More” link is clicked on the Incognito splash screen.<sup>35</sup> Respondents were forced to view this screen for an additional 30 seconds.<sup>36</sup>
73. This sequence of forced exposures is not realistic of the way that most consumers interact with Chrome in Incognito mode. With repeated use and exposure to the Incognito splash screen, it is unlikely that any user would spend 30 seconds studying the limited information presented on that page. Most users quickly proceed to executing the search or navigating to the URL for which they opened a Chrome Incognito window. Indeed, in the Keegan Study, respondents’ median viewing times for the browser splash screens were 8.9 seconds for Chrome, 9.1 seconds for Safari, and 10.1 seconds for Edge/Internet Explorer.
74. Additionally, the study’s forced 30 second exposure to the “Learn more” page for all respondents is unrealistic: another of the Amir Studies—the Likelihood of Use Study—proves that exceedingly few users (just 2.4 percent of respondents) even click on the Learn More link (discussed below). In light of this information, forcing respondents in the

---

<sup>34</sup> Amir Report Appendices, p. F.1-7.

<sup>35</sup> Amir Report Appendices, p. F.1. This was not the actual “Learn More” page that Google uses, but a deeper-linked page that requires an extra click to access. The actual screen currently displayed when “Learn More” is clicked ([https://support.google.com/chrome/answer/9845881?visit\\_id=6378780186528342754248452860&p=incognito&rd=1](https://support.google.com/chrome/answer/9845881?visit_id=6378780186528342754248452860&p=incognito&rd=1)) was not used in the study. Rather, another page ([https://support.google.com/chrome/answer/7440301?hl=en&ref\\_topic=9845306](https://support.google.com/chrome/answer/7440301?hl=en&ref_topic=9845306)), presumably considered more favorable to Google’s position in this case, was asserted as the page that respondents would see upon clicking the “Learn More” link on the Incognito splash screen. This page is not currently accessible directly from the Incognito splash screen.

<sup>36</sup> Amir Report Appendices, p. F.1.

Consumer Perceptions and Expectations Study to study Google’s Learn More disclosures is not reflective of the realities of an actual use case. Hence, any measurements that come from this unrealistic scenario do not measure actual user beliefs.

***Irrelevant variables – unclear entities***

75. The Consumer Perceptions and Expectations Study purports to measure what PBM users “expect while in private browsing mode.”<sup>37</sup> In an attempt to collect this information, the survey asks respondents if three different types of entities receive different types of information while they are privately browsing. The entities inquired about, without further explanation to respondents, are presented as follows:
  - a. “Companies that own the websites that you visited during the session”
  - b. “Your internet service provider”
  - c. “Companies that provide analytics and advertising services to websites you visited during the session”
76. The entities presented to respondents in the Consumer Perceptions and Expectations Study do not comport with the allegations in this case. The Consumer Perceptions and Expectations Study claims to have used “more understandable concept[s]”<sup>38</sup> when interpreting the Complaint allegations and presenting those to respondents. However, this attempt fails as the study does not accurately convey the Complaint allegations to respondents, and in some cases omits allegations completely. The Consumer Perceptions and Expectations Study therefore measures something wholly irrelevant.
77. The Consumer Perceptions and Expectations Study has the effect of obfuscating what consumers’ actual perceptions and expectations are with regard to the collection and use of the types of information and data that is at issue in this matter. Most notably, the reader is never asked whether Google collects information, or whether the user understands that Google is the company that provides analytics and advertising services to websites and thereby collects users’ PBM data. Given this critical omission, the reader does not know—

---

<sup>37</sup> Amir Report Appendices, p. G.1-11.

<sup>38</sup> Amir Report, p. 10.



and survey respondents themselves are given no guidance—on what “Companies that provide analytics and advertising services to websites you visited during the session” means. Is this referencing all such companies, of which there are many? Certain of these companies? All companies except Google? Only Google? It is impossible to know. As a consequence, respondents are left to interpret this ambiguous language in their own varied ways.

78. Additionally, the allegations in the Complaint with respect to the collection of users’ information is confined to the activities and practices of Google; however, the Consumer Perceptions and Expectations Study makes no such restriction regarding consumer perceptions and expectations when using PBM. Indeed, Google is not mentioned as an entity at all.
79. Because the Consumer Perceptions and Expectations Study asks respondents to consider what may be received by the three ambiguous types of entities described above, and not Google specifically, the measurement derived from this faulty methodology cannot be reliably applied to the allegations against Google alone in this case.

***Irrelevant variables – oversimplification of data types***

80. In addition to the misalignment of the three categories of entities in the Consumer Perceptions and Expectations Study to the allegations, the three types of information inquired about are also misidentified. The three types of information asked about are presented to respondents as:
  - a. “IP addresses,” defined as “Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. An IP address can often be used to identify the location from which a device is connecting to the Internet.”<sup>39</sup>
  - b. “URLs of the sites you visit,” defined as “The web addresses of the webpages you visited using the browser.”<sup>40</sup>
  - c. “Cookies,” defined as “A small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the

---

<sup>39</sup> Amir Report, p.10.

<sup>40</sup> Amir Report, p.10.

cookie allows that site to recognize your browser. Cookies may store user preferences and other information.”<sup>41</sup>

81. Although the Complaint makes clear that Google surreptitiously collects and saves many categories of information from users while in PBM,<sup>42</sup> the Consumer Perceptions and Expectations Study erroneously oversimplifies its description of this activity to respondents, consolidating all such data collection under the inaccurate umbrellas of “IP addresses,” “URLs of the sites you visit,” and “Cookies.”<sup>43</sup> This is a gross oversimplification considering that the Third Amended Complaint alleges many categories of user information that is passed along to Google without the users’ knowledge.<sup>44</sup>
82. Additionally, while acknowledging certain allegations, the Amir Study fails to include them at all. For example, “fingerprint data” is one of the types of information alleged to be collected by Google while users are private browsing,<sup>45</sup> and is listed as such in the Amir Report,<sup>46</sup> yet the Amir Study omits it entirely from its list of types of information communicated.<sup>47</sup> This is also the case for “User-ID” data.<sup>48</sup>
83. The Consumer Perceptions and Expectations Study fails to properly encompass the entirety of the allegations in this case and communicate those to respondents in the study. The study therefore does not faithfully measure pertinent information that can be applied to the allegations against Google in this matter.

---

<sup>41</sup> Amir Report, p. 11.

<sup>42</sup> Third Amended Complaint, pp. 17-18.

<sup>43</sup> Some of the Complaint allegations regarding the types of information collected and saved are relabeled or consolidated in the Consumer Perceptions and Expectations Study. For example, “GET requests” become “URLs”, with the explanation that “I am informed that ‘URLs of the sites visited’ is a more understandable concept for survey respondents. Thus, I presented the term, ‘URLs of the sites you visit’ (Amir Report, FN19). The rebranding of this allegation to respondents fails to accurately convey the type of information being collected by Google. Such mischaracterization ultimately leads to a failure to accurately measure consumer perceptions and expectations regarding the allegations.

<sup>44</sup> Third Amended Complaint, pp. 17-18.

<sup>45</sup> Third Amended Complaint, p. 18.

<sup>46</sup> Amir Report, p. 10.

<sup>47</sup> Amir Report, p. 23.

<sup>48</sup> Amir Report, p. 10.

***Summary – Consumer Perceptions and Expectations Study***

84. The Consumer Perceptions and Expectations Study is hampered by a number of material deficiencies and limitations, including:
- Use of a biased reading test survey format which makes the survey stimuli available to respondents during the administration of key study measures;
  - Failure to replicate the marketplace because of the use of lengthy forced exposures to Google and other private browsing disclosures; and
  - Use of irrelevant variables which do not accurately convey the Complaint allegations to respondents, and in some cases omit allegations completely.
85. For these reasons, the Consumer Perceptions and Expectations Study provides no valid or reliable evidence regarding the perceptions, expectations, beliefs, or behaviors of any reasonable Class Member with respect to Google’s PBM data collection and storage practices. As such, the Interpretation Study provides no support for Professor Amir’s stated opinions with respect to any Class Members.

***Interpretation Study***

86. The Interpretation Study was purportedly intended “to assess whether and to what extent users expect Google to receive or to not receive URLs of the sites users visit, IP addresses, and cookies placed on users’ browsers during their Incognito session after reviewing the Incognito Splash Screen and ‘Learn More’ page” as well as various other disclosures.<sup>49</sup> In addition to the deficiencies and limitations identified above, the following sections discuss additional deficiencies and limitations of this study.

***Failure to replicate the market***

87. Like the Consumer Perceptions and Expectations Study, the Interpretation Study fails to replicate the ways in which potential Class Members interact with and use PBM. Because the Interpretation Study fails to replicate the marketplace, it does not yield valid and reliable data upon which opinions and conclusions can be drawn about any Class Members.

---

<sup>49</sup> Amir Report, ¶ 8.

88. The main portion of the Interpretation Study began by assigning respondents to one of four groups, each of which was exposed to different study stimuli. The stimuli assignments for the four groups were defined as follows:<sup>50</sup>

	<b>Number of Completes</b>	<b>Stimuli Description</b>
GROUP A (Splash Screen Only)	250	<ul style="list-style-type: none"> <li>• Incognito Splash Screen</li> <li>• “Learn More” page</li> </ul>
GROUP B (Splash Screen with Policies (Highlighted))	250	<ul style="list-style-type: none"> <li>• Google Privacy Policy, March 31, 2020 (with and without highlights)</li> <li>• Chrome Privacy Notice, May 20, 2020 (with and without highlights)</li> <li>• Incognito Splash Screen</li> <li>• “Learn More” page</li> </ul>
GROUP C (Splash Screen with New Account Creation Agreement)	250	<ul style="list-style-type: none"> <li>• New Account Creation Agreement</li> <li>• Incognito Splash Screen</li> <li>• “Learn More” page</li> </ul>
GROUP D (Splash Screen with Consent Bump Agreement and FAQ Page)	250	<ul style="list-style-type: none"> <li>• Consent Bump Agreement and FAQ page</li> <li>• Incognito Splash Screen</li> <li>• “Learn More” page</li> </ul>

89. As shown in the table above, respondents in the Interpretation Study were forced to review up to four Google disclosures discussing various aspects of its data collection practices with respect to PBM. From the outset, this is an unrealistic exercise: the Amir Likelihood of Use Study proves that exceedingly few users—just 2.4 percent of respondents—click on the Learn More link (discussed below), yet a lengthy exposure to this information was required for all users in this study.
90. The artificial nature of this exercise cannot be overstated. The Interpretation Study’s stimuli exposures do not in any way replicate the experience that a typical user would have when

---

<sup>50</sup> Amir Report Appendices, p. F.2-6.

using Chrome Incognito. For example, respondents assigned to Group B were first exposed to Google's Privacy Policy, which they were forced to review for at least 30 seconds.<sup>51</sup> On the next page, respondents were forced to again view the Google Privacy Policy—this time with certain portions highlighted—for an additional 15 seconds.<sup>52</sup> Next, respondents were forced to view the Chrome Privacy Notice for at least 30 seconds.<sup>53</sup> On the next page, respondents were forced to again view the Chrome Privacy Notice—this time with highlights—for an additional 15 seconds.<sup>54</sup> Respondents were next forced to view the Chrome Incognito splash screen for at least 30 seconds.<sup>55</sup> Finally, respondents were forced to view a page characterized as the Incognito “Learn More” page for at least 30 seconds.<sup>56</sup>

91. The Interpretation Study's stimuli exposure scheme is simply not reflective of the way that typical users engage with Chrome Incognito in a natural environment. In total, respondents in this group were forced to review six Google disclosures over a timespan of no less than two and a half minutes before answering any key study measures (while once again providing those respondents with copies of all of those disclosures while answering questions, employing a forced “reading test” format). This stands in contrast to the Keegan Study, wherein with no minimum forced exposure time, respondents' median viewing times for the browser splash screens were 8.9 seconds for Chrome, 9.1 seconds for Safari, and 10.1 seconds for Edge/Internet Explorer.
92. It is highly unlikely that any respondent seeking to use Chrome Incognito would spend multiple minutes reviewing multiple Google disclosures before engaging in private browsing. Among those that do review one or more Google disclosures, is unlikely that such users would review all of those disclosures in direct succession.

---

<sup>51</sup> Amir Report Appendices, p. F.2-8.

<sup>52</sup> Amir Report Appendices, p. F.2-9.

<sup>53</sup> Amir Report Appendices, p. F.2-10.

<sup>54</sup> Amir Report Appendices, p. F.2-11.

<sup>55</sup> Amir Report Appendices, p. F.2-15.

<sup>56</sup> Amir Report Appendices, p. F.2-16.

***Leading questions***

93. The Interpretation Study is also problematic insofar as the survey instructions and questions unnaturally lead respondents to information and answers that are beneficial to Google. A leading question is a question that, through the methodological construction of the question itself, suggests to the respondent particular information and/or a particular answer. It has been noted that “in framing survey questions, one must resist the temptation to lead responses to a desired end or to ‘help’ the witness to reach the ‘correct’ answer.”<sup>57</sup> Leading questions “may threaten the validity of the survey by systematically distorting responses if respondents are misled in a particular direction.”<sup>58</sup>
94. The inclusion of highlighted passages in the study stimuli is a particularly perplexing example of this. Not only is highlighting content a complete fabrication that would not occur in the natural marketplace—i.e., users would never be exposed to highlighted passages when using Chrome Incognito outside of the Interpretation Study—but the use of highlights effectively cues respondents to focus on the exact content that Google wants them to review, and which may in turn cause respondents to disregard other portions of the documents that are not helpful to Google. This is a material deficiency of the Interpretation Study: to the extent that the highlighted content impacts the ways in which respondents review and process the information presented in Google’s disclosures, this design choice biases respondents’ understanding of Google’s PBM data collection and storage practices.
95. The Interpretation Study also made use of unclear and leading language in the survey instructions and questions, which contributes to respondents’ potentially unnatural review of the Google disclosures. For example, the Interpretation Study potentially biases respondents at the outset of the key study measures by directly linking Google and Chrome. Respondents are instructed, “You have been selected to answer questions about Chrome, which is a browser from a company named Google.”<sup>59</sup> [Emphasis in original.] The Interpretation Study’s effort through this instruction to establish a link between Google and Chrome potentially conditions respondents to focus on the information that *Chrome* stores locally on

---

<sup>57</sup> McCarthy, T.J. (2020). *McCarthy on Trademarks and Unfair Competition*, 5<sup>th</sup> Ed, §32:173.

<sup>58</sup> Diamond, S. (2011). “Reference Guide On Survey Research,” in *Reference Manual on Scientific Evidence*. Federal Judicial Center/National Academy of Sciences, p. 388.

<sup>59</sup> Amir Report Appendices, p. F.2-7.

one's computer, as opposed to the relevant issue in this case, which I understand to be *Google's* remote collection and storage of PBM data.

96. Additionally, before viewing the study stimuli, respondents were told that they “will be able to view these images again as you answer the questions.”<sup>60</sup> Respondents were instructed to read through the stimuli “carefully” and were repeatedly told that the stimuli would be available to view when answering questions. For all three of the key study measures, respondents were told to answer “based on the screens you reviewed.”<sup>61</sup>
97. Because the leading nature of the Interpretation Study's questionnaire potentially impacted the Interpretation Study's data in unknown ways, the reliability of the study's data is undermined.
98. The study instructions also contribute to respondents' unnatural review of the Google disclosures. Throughout the Interpretation Study, respondents are provided with the following instructions which place undue emphasis on Google's disclosures:
  - “You will now see the Google Privacy Policy. Please carefully read this policy...Please scroll through the window below to see the whole image.”<sup>62</sup>
  - “You will be able to view these images again as you answer the questions”<sup>63</sup>
  - “Please carefully read this policy”<sup>64</sup>
  - “Please scroll through the window below to see the whole image”<sup>65</sup>
  - “The thumbnails contain the images that you have viewed earlier. You can click on the thumbnails to see the enlarged versions of these images.”<sup>66</sup>

---

<sup>60</sup> Amir Report Appendices, p. F-2.7.

<sup>61</sup> Amir Report Appendices, pp. F.2-17 - F.2-19.

<sup>62</sup> Amir Report Appendices, p. F.2-8.

<sup>63</sup> Amir Report Appendices, p. F.2-7.

<sup>64</sup> Amir Report Appendices, p. F.2-8.

<sup>65</sup> Amir Report Appendices, p. F.2-9.

<sup>66</sup> Amir Report Appendices, p. F.2-17.



99. The Interpretation Study primes respondents to study Google's disclosures in ways that are not reflective of reality. The leading nature of the questionnaire language undermines the reliability of the Interpretation Study's data and the opinions and conclusions drawn therefrom.

***Irrelevant variables – oversimplification of data types***

100. Like the Consumer Perceptions and Expectations Study, the Interpretation Study also oversimplifies the types of data that are collected by Google when a user searches the Internet in PBM. Here again, the Interpretation Study consolidates all of Google's data collection activities under the inaccurate umbrellas of "IP addresses," "URLs of the sites you visit," and "Cookies."<sup>67</sup> For this reason, with respect to its oversimplification of the types of data collected by Google when a user searches the Internet in PBM, the Interpretation Study is subject to the same critiques as the Consumer Perceptions and Expectations Study as outlined above.

***Inappropriate reading test***

101. The Interpretation Study bears the hallmarks of a classic reading test. As such it is inherently biased and cannot be considered reliable evidence in this matter.
102. As discussed above, each of the four study groups was subjected to an extended forced exposure to their assigned stimuli. After this forced exposure, three key measures were administered:
- Based on the screens that you reviewed, please select one of the following regarding URLs of the sites you visit during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product);<sup>68</sup>
  - Based on the screens that you reviewed, please select one of the following regarding IP address during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product);<sup>69</sup> and

---

<sup>67</sup> Amir Report Appendices, pp. F.2-17, F.2-18.

<sup>68</sup> Amir Report Appendices, p. F.2-17.

<sup>69</sup> Amir Report Appendices, p. F.2-18.

- Based on the screens that you reviewed, please select one of the following regarding cookies placed on your browser during an Incognito mode internet browsing session (e.g., watching a video or shopping for a product).<sup>70</sup>

103. Each of the three measures employed a five-point scale ranging from “Google does not receive this information” to “Google does receive this information.” An additional answer option—I don’t feel I have enough information to answer this question—was provided for each of the three measures.
104. For each of the questions of interest, the Interpretation Study allowed respondents access to the stimuli that they had viewed when answering the question. For all of the questions of interest, respondents were instructed that there are thumbnails on the page that “contain the images that you have viewed earlier”<sup>71</sup> and that they “can click on the thumbnails to see the enlarged versions of these images.”<sup>72</sup>
105. Respondents are also told to answer the questions “based on the screens that you reviewed.”<sup>73</sup> This instruction places undue emphasis on the study stimuli and potentially conditions respondents to answer the questions in ways that they would not in the absence of such an instruction.
106. For these reasons, the Interpretation Study is subject to the same critiques as the Consumer Perceptions and Expectations Study as outlined above with respect to its use of a reading test format.

### ***Summary – Interpretation Study***

107. The Interpretation Study is hampered by a number of material deficiencies and limitations, including:
- Failure to replicate the marketplace because of the use of lengthy forced exposures to Google’s disclosures;

---

<sup>70</sup> Amir Report Appendices, p. F.2-18.

<sup>71</sup> Amir Report Appendices, p. F.2-17.

<sup>72</sup> Amir Report Appendices, p. F.2-17.

<sup>73</sup> Amir Report Appendices, pp. F.2-17, F.2-18.

- Use of survey instructions and questions unnaturally lead respondents to information and answers that are beneficial to Google;
- Oversimplification of the types of data that are collected by Google when a user searches the Internet in PBM; and
- Use of a biased reading test survey format which make the survey stimuli available to respondents during the administration of key study measures.

108. For these reasons, the Interpretation Study provides no valid or reliable evidence regarding the perceptions, expectations, beliefs, or behaviors of any reasonable Class Member with respect to Google's PBM data collection and storage practices. As such, the Interpretation Study provides no support for Professor Amir's stated opinions with respect to any Class Members.

#### **Likelihood of Use Study**

109. The Likelihood of Use Study was purportedly intended "to assess whether and to what extent modification of certain language on the Incognito Splash Screen and the 'Learn More' page that address Plaintiffs' criticisms of those documents...impacts users' likelihood of using Chrome in Incognito mode for private browsing."<sup>74</sup> In addition to the deficiencies and limitations identified above, the following sections discuss additional deficiencies and limitations of this study.

#### ***Flawed disclosure modifications***

110. The Likelihood of Use Study purported to measure the impact of alternate language presented to users when private browsing. Using a test vs. control design, one group of respondents saw a Chrome Incognito splash screen in its unaltered state, whereas a second group of respondents saw a Chrome Incognito splash screen with alternative language. The unaltered "Learn More" page and a modified alternative language version were also made available to these respective groups.<sup>75</sup>

---

<sup>74</sup> Amir Report, ¶ 13.

<sup>75</sup> Amir Report, ¶ 77.

Actual Language Group	Alternative Language Group
<ul style="list-style-type: none"> <li>• Actual Chrome Incognito Splash Screen</li> <li>• <i>(If respondent clicked the “Learn more” hyperlink)</i> Actual “Learn More” page</li> </ul>	<ul style="list-style-type: none"> <li>• Alternative Chrome Incognito Splash Screen</li> <li>• <i>(If respondent clicked the “Learn more” hyperlink)</i> Alternative “Learn More” page</li> </ul>

111. By comparing the self-reported anticipated usage behaviors of these two groups, the study claims to have measured the impact of the alternative language on respondents’ “likelihood that they would use Chrome in Incognito mode to do online research.”<sup>76</sup>

112. The Amir Report asserts that “these language modifications address Plaintiffs’ allegations as to how the actual language in the Incognito Splash Screen allegedly is misleading.”<sup>77</sup> However, the fundamental premise of this test—that the alternative language stimulus represents a proper disclosure to respondents—is flawed, dooming this exercise from the outset.

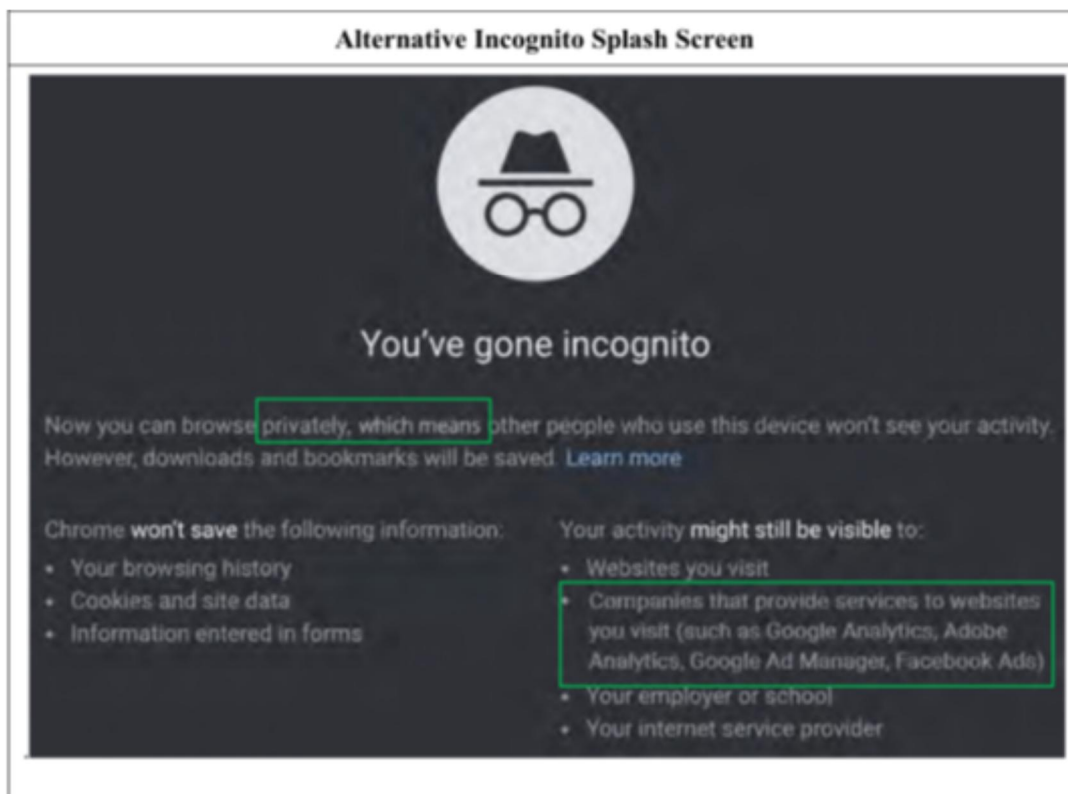
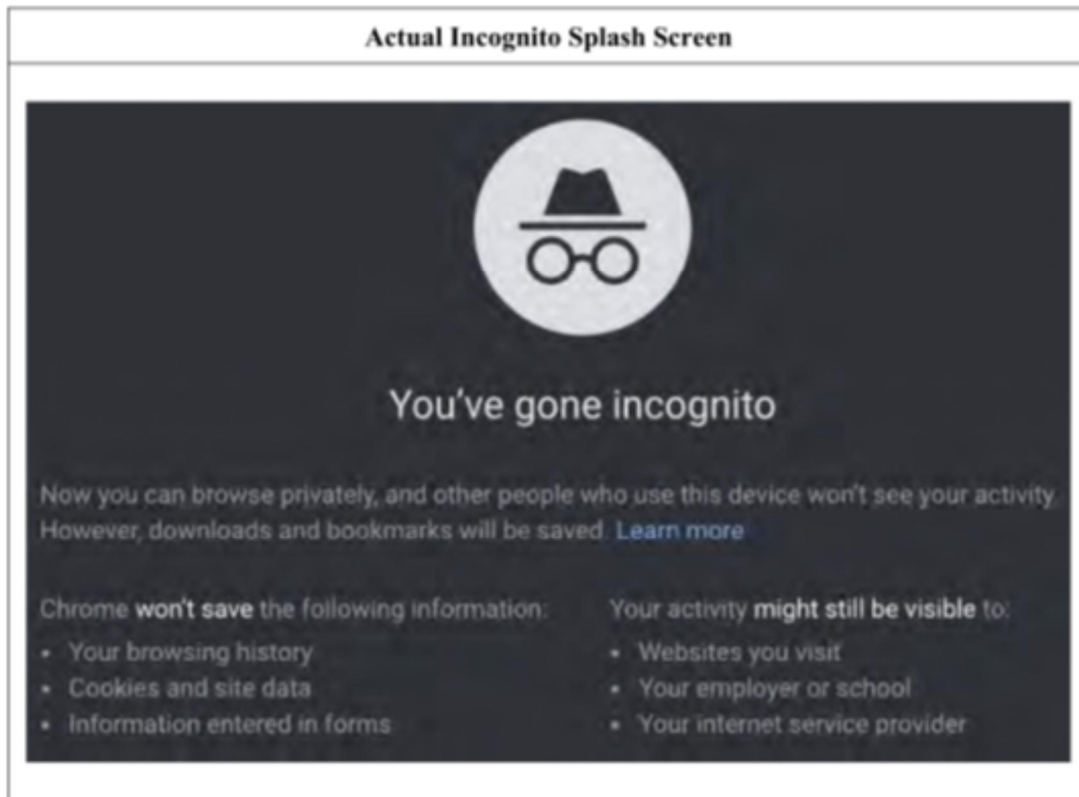
113. As shown below, just two minor modifications were made to the Incognito splash screen to arrive at the alternative language version: (1) alteration of the top disclosure statement; and (2) the addition of a bullet point.<sup>78</sup>

---

<sup>76</sup> Amir Report, p. 39.

<sup>77</sup> Amir Report, p. 38.

<sup>78</sup> Amir Report, p. 38.



114. Considering first the top disclosure statement, the unaltered Incognito splash screen used in the study reads:

Now you can browse privately, **and** other people who use this device won't see your activity. [Emphasis added.]

115. The modified Incognito splash screen reads:

Now you can browse privately, **which means** other people who use this device won't see your activity.<sup>79</sup> [Emphasis added.]

116. The second and final modification to the test Incognito screen was the addition of a seventh informational bullet point. The modified Incognito screen added a seventh bullet in the middle of the right-hand list titled "Your activity might still be visible to," that reads:

- Companies that provide services to websites you visit (such as Google Analytics, Adobe Analytics, Google Ad Manager, Facebook Ads).<sup>80</sup>

117. This "further clarifying" language does no such thing. The Incognito page language "You've gone incognito" and "Now you can browse privately" and use of "disguise" iconography<sup>81</sup> communicates (as demonstrated by the Keegan Study, and as confirmed by Google's own internal documents<sup>82</sup>) a clear message of privacy to users that is alleged to be misaligned with the actual lack of privacy afforded. The meager additional language provided in the alternative language group stimulus does not appear to be sufficient to overcome the overall communication of tracking-free browsing that consumers are alleged to expect and, according to the Keegan Study and Google's own documents, do expect.

118. Additionally, the added bullet point appears under the innocuous heading of "Your activity might still be visible to." The extent to which, if at all, consumers are cognizant that "visible" actually means collected, stored and used by Google for purposes beyond simply providing

---

<sup>79</sup> Amir Report, p. 37.

<sup>80</sup> Amir p. 37.

<sup>81</sup> Third Amended Complaint, p. 14.

<sup>82</sup> See "Analysis of Google Internal Documents" section below; See also Exhibit 8.

services for websites that users visit in PMB cannot be determined from the Likelihood of Use Study.

119. The Amir Report assumes, without any support, that the language added to the alternative language page solves all the Google disclosure issues to which the Plaintiffs object.<sup>83</sup> However, consumers' impressions of what this language communicates is never measured. What was measured was the "likelihood that [respondents] would use Chrome in Incognito mode to do online research on a sensitive topic on a scale of 1 (Unlikely) to 5 (Likely)."<sup>84</sup> The likelihood of use measurement tells the reader nothing about what the alternative language communicates or does not communicate.
120. The Likelihood of Use Study could have measured what the alternative language communicated to respondents separate and apart from the unaltered language by asking, for example, about respondents' beliefs regarding Google's collection of their browsing activity. This was not done.

***Failure to account for confounding variables***

121. Additionally, using the indirect measurement of respondents' "likelihood of using" Chrome Incognito ignores a range of confounding variables which obfuscate the impact, if any, of the alternative language. Perhaps, for example, users in the alternative language group are alarmed to learn that their PBM browsing activity is visible to Google Analytics but would still use Incognito at the same rate because it is convenient. Other users might have negative feelings about Google collecting and saving their private browsing data but are required to continue using Chrome on a work or school computer or to access certain websites.<sup>85</sup>

---

<sup>83</sup> It is also notable that the language changes made by Professor Amir are inconsistent with proposed changes that Google's own employees considered in 2021 to address known user misconceptions regarding Chrome Incognito mode, as referenced in Exhibit 8. For example, in 2021 it was recommended internally that Google remove the language "Now you can browse privately" entirely from the Incognito Splash Screen, noting that "the word 'private'" poses "the risk of overestimating the protection Incognito offers" (GOOG-CABR-04746153 at -172).

<sup>84</sup> Amir Report, p. 39.

<sup>85</sup> Expert Report of Bruce Schneier, 4/15/2022, ¶¶ 169-171.



122. Indeed, countless potential scenarios could account for the consumer decision to continue using Chrome Incognito that are not based in privacy concerns.<sup>86</sup> What is not known from the Likelihood of Use Study design is *why* users are unlikely or likely to use Chrome Incognito and whether this has anything to do with the modest alternative language presented in the study. Nor does the Likelihood of Use Study provide any information about consumers' feelings, either positive or negative, about Google's PBM data collection and storage practices.

***Self-serving "Learn More" exposure***

123. The Likelihood of Use Study also employs a methodological element which improperly weighs the survey findings in favor of Google. In the first two Amir Studies (Consumer Perceptions and Expectations Study and Interpretation Study), respondents were forced to view the "Learn More" page regardless of whether they would have chosen to do so on their own.<sup>87</sup> In the Likelihood of Use Study, however, respondents have the choice whether to click on the Learn More link and view additional information about Google's PBM data collection and storage practices. These methodological choices advantage a favorable outcome for Google across all three Amir Studies:

- In the first two studies, wherein the studies are designed to collect information about respondents' *knowledge* about Google's PBM data collection practices (improperly measured by a reading test), the methodologies require that respondents view the information on the Learn More page *because a more informed respondent yields a better result for Google on these measures*.
- In the Likelihood of Use Study, wherein the study is designed to collect information about whether respondents *will continue using* Chrome Incognito after being exposed to the actual or alternative language Incognito splash screens, the methodology makes exposure to the Learn More screen optional *because a less informed respondent yields a better result for Google on this measure*.

124. By employing a test vs. control design, the Likelihood of Use Study seeks to determine whether there is a difference in respondents' likelihood of using Chrome Incognito depending on the stimulus viewed (actual language vs. Likelihood of Use Study alternative language).

---

<sup>86</sup> As Professor Amir states in his report, "consumer preferences vary when it comes to internet browsers and browser features, and consumers' concerns about privacy vary depending on context." Amir Report, p. 21.

<sup>87</sup> Professor Amir's Likelihood of Use Study shows that very few respondents—2.4 percent—actually click the "Learn More" page when given the choice.

Because there are so few differences between the two splash screens, it is perhaps not surprising that there would be little difference between respondents' likelihood of continuing to use Chrome Incognito between the two groups.

125. Making the Learn More screens optional serves as a mechanism to limit the number of respondents that receive additional disclosure as to Google's data collection practices before indicating their likelihood of continuing to use Chrome Incognito. The data from the Likelihood of Use Study confirms this trend: of the 1,005 respondents who participated in the study, just 24—2.4 percent—clicked on the Learn More link, showing that this information was virtually unseen by respondents in the test or the control.<sup>88</sup> So while the study purports to expose test and control groups to varying levels of disclosures, the study design in effect creates conditions for the two groups that are largely identical, ensuring the reported results.

***Summary – Likelihood of Use Study***

126. The Likelihood of Use Study is hampered by a number of material deficiencies and limitations, including:

- Failure to create a consumer disclosure that sufficiently or effectively communicates the level of Google data collection alleged in the Complaint, let alone address any of the storage and usage issues;
- Ignoring confounding variables and hence failing to generate reliable information regarding what, if anything, the alternative language communicates to respondents; and
- Presenting respondents with a self-serving optional exposure to the “Learn More” page—in contrast to forced exposure in the other two Amir Studies—which serves to limit the actual alternative disclosures seen by respondents and therefore weighs the results in favor of the Google by reducing any potential impact on the results.

127. For these reasons, the Likelihood of Use Study provides no valid or reliable evidence regarding the perceptions, expectations, beliefs, or behaviors of any reasonable Class Member with respect to Google's PBM data collection and storage practices. As such, the

---

<sup>88</sup> Likelihood of Use Study data file, 2203523.xlsx.

Likelihood of Use Study provides no support for Professor Amir's stated opinions with respect to any Class Members.

### **Conclusions – Amir Report**

128. The three studies presented in the Amir Report are hampered by numerous methodological and analytical flaws, as described above.
129. The three studies presented in the Amir Report do not comprise reliable and valid evidence with respect to consumer beliefs or expectations regarding Google's data collection practices while in private browsing mode.
130. As such, any opinions and conclusions presented in the Amir Report that are based on the findings of the Amir Studies are unsupported.

## **V. The Keegan Study**

### **Summary of assignment**

131. In light of the material methodological and analytical limitations of the Amir Studies, I was asked to design and execute a methodologically sound rebuttal survey—responsive to the Amir Studies—to reliably measure consumer perceptions and expectations with regard to Google's PBM data collection and storage practices, specifically, the extent to which Google collects and saves the user's personal information when using PBM.
132. To this end, I designed and executed a nationally representative U.S. study of 1,052 users of PBM in the Internet browsers relevant to the allegations in this matter (Chrome, Safari, and/or Edge/Internet Explorer) during the Class Period. Qualifying respondents were asked a series of questions to determine the extent to which they understand (or misunderstand, according to the allegations) Google's practices with regard to collecting and saving user data during PBM sessions.
133. My study addressed and corrected many errors in the Amir Studies, including:
- a. Correcting Professor Amir's browser selection error (where the Amir Studies concern Chrome, Safari, and Firefox, and Plaintiffs seek to represent users of Chrome, Safari, and Edge/Internet Explorer);

- b. Correcting Professor Amir's time period selection error (where Amir selected six months and I used five years);
- c. Correcting Professor Amir's problematic use of forced viewing time periods for study stimuli;
- d. Correcting Professor Amir's problematic use of available study stimuli on the same pages as key study measures;
- e. Correcting Professor Amir's presentation of materials that would not otherwise have been presented to users when starting private browsing;
- f. Correcting Professor Amir's failure to ask any questions regarding Google saving information collected when users are in PBM;
- g. Correcting Professor Amir's failure to ask any questions about whether people believed they had consented to Google's PBM data collection and storage practices;
- h. Correcting Professor Amir's failure to ask any questions about whether people believed they had consented to Google's PBM data collection and storage practices when visiting non-Google websites; and
- i. Correcting Professor Amir's failure to ask any questions about whether people believed they had consented to Google's PBM data collection and storage practices when visiting non-Google websites while not logged in to a Google account.

134. As discussed in detail below, unlike the Amir Studies, my study conforms to best practices of survey research, and accordingly, reflects far different results than the Amir Studies. All findings are presented with a reasonable degree of scientific certainty.

135. The methodology and results of my study are presented in detail in the sections that follow.

**Methodology*****Study integrity***

136. This study of 1,052 U.S. respondents was designed and executed in accordance with accepted standards of survey research. This survey follows the guiding principles for survey research for the purpose of litigation as outlined by Shari Diamond,<sup>89</sup> including but not limited to:

- Appropriate universe selection and sampling frame;
- Rigorous and valid survey design that is probative of the relevant issues in the matter;
- Inclusion of representative, qualified respondents;
- Use of procedures to minimize potential biases in data collection;
- Use of objective, non-leading questions;
- Use of procedures to reduce guessing among respondents; and
- Full analysis and reporting of survey data.

137. Additional treatises commonly referenced by researchers conducting survey research for litigation were also instrumental in the design of the current research.<sup>90</sup>

***Study objectives***

138. The primary objective of this study was to design and execute valid and reliable survey evidence, responsive to the Amir Studies, on the issue of the perceptions and expectations of potential Class Members regarding Google's PBM data collection and storage practices, specifically, the extent to which Google collects and saves the user's personal information when using PBM.

---

<sup>89</sup> Diamond, S. (2011). "Reference Guide On Survey Research," in *Reference Manual on Scientific Evidence*. Federal Judicial Center/National Academy of Sciences, p. 359-423.

<sup>90</sup> See, for example, McCarthy, J.T. (2020). *McCarthy on Trademarks and Unfair Competition*, 5<sup>th</sup> Ed.; Jacoby, J. (2013). *Trademark Surveys, Volume 1: Designing, Implementing, and Evaluating Surveys*.

139. The purpose of this study was to correct for the deficiencies and limitations of the Amir Studies and to thereby generate more valid and reliable evidence addressing the issues relevant to this matter.

***Study population***

140. Surveys are conducted by collecting data from a sample, or subset, of the population of interest, i.e., the larger group to which the study results may be projected. This survey is intended to provide information relevant to the proportion of U.S. respondents who may be Class Members—i.e., the population of U.S. consumers who engage in Internet browsing and have used one or more of the relevant private browsing modes during the past five years and may meet the requirements to be included in the prospective Classes. This stands in contrast to the Amir Studies, which sampled only from those users who had engaged in private browsing within the last six months (after the lawsuit was filed).

141. Consistent with typical marketing research practice, only respondents aged 18 and older were permitted to participate in the study.<sup>91</sup> Respondents who met the study population definition were identified through the use of screening questions that qualified respondents on these criteria (see Questionnaire at Exhibit 3).

***Study design***

142. Unlike the Amir Studies, which primed respondents through forced exposures to disclosures and measured their ability to read back information from those disclosures, this study was designed to gauge respondents' actual, non-conditioned understanding of Google's PBM data collection and storage practices.

143. After qualifying respondents through a screening module and exposing them to the PBM splash screen for their browser assignment (discussed below), the main portion of the study asked respondents questions pertaining to the following issues:

- Whether users believe that Google collects and saves Internet browsing activity when the user browses the Internet in PBM;

---

<sup>91</sup> Special procedures and precautions must be followed when interviewing minors (see ESOMAR Guideline on Interviewing Children and Young People, [www.esomar.org](http://www.esomar.org)). For this reason, it is typical to interview minors only when there is a specific reason to do so. There was no such reason here.

- Whether users believe they have given consent for Google to collect and save information about their Internet browsing activity when in PBM;
- Whether users believe they have given consent for Google to collect and save information about their Internet browsing activity when visiting a non-Google website when in PBM;
- Whether users believe they have given consent for Google to collect and save information about their Internet browsing activity when they are signed out of their Google account when in PBM; and
- Whether users believe that Google collects and saves various specific types of browsing data (discussed below) when in PBM.

144. The Class Period begins June 1, 2016. The past five-year period was used in my survey to simplify the presentation to respondents rather than asking them to recall whether the specifics of a casual event—Internet browsing—occurred five years ago or five years and ten months ago.

145. Consistent with standard marketing research practice, several demographic questions were also administered.

### ***Data collection***

146. This survey was completed through online interviewing via the Internet. Online interviewing is the dominant data collection method used in marketing research today.<sup>92</sup> Data collection for this study took place in May 2022.

147. The respondent sample for this project was provided by the Dynata<sup>93</sup> consumer panel. Dynata is a leading provider of online sample for research projects in the U.S. and across the globe. Dynata maintains an actively managed online panel of millions of consumers. Membership in the panel is by invitation only, and Dynata employs and enforces a range of policies and procedures to ensure “panel health”—i.e., that the panel is nationally representative and that

---

<sup>92</sup> *Global Market Research 2021: An ESOMAR Industry Report*, p. 58-61.

<sup>93</sup> [www.dynata.com](http://www.dynata.com).



respondents provide honest and accurate answers to questions. Additional panel health checks include participation limits, screening questions, digital fingerprinting, IP verification, anti-automation filtering, random and illogical responding, capturing and removing flatliners and speeders, among others. Dynata utilizes a “double opt-in” procedure in its recruitment process, which helps to verify the respondent’s identity and ensure the panel is populated by quality participants.<sup>94</sup>

148. I have personally used Dynata as a sample provider for many consumer research studies, am familiar with its panel health procedures, and am satisfied that it provides high quality, representative respondents. The Dynata consumer panel constituted the sampling frame of the study.

149. The survey was programmed using Qualtrics, an industry-leading online survey software platform. All survey programming was performed by Keegan & Donato Consulting. The survey software facilitates the programming and execution of advanced survey designs, custom coding, complex skip logic, and advanced rotation and randomization of questions, answer options, and stimuli. All such options were employed wherever appropriate.

### ***Sampling***

150. Surveys typically, and in this case, are designed such that the results are reliable at the 95 percent confidence level. A total of 1,052 respondents qualified for and completed the questionnaire (see full disposition of contacts at Exhibit 7). Samples of this size are associated with a maximum margin of error of  $\pm 3.0$  percentage points at 95 percent confidence.<sup>95</sup>

### ***Bias management***

151. All efforts were made to present the survey questions in an objective, unbiased, and non-leading format. Respondents were presented with a “don’t know,” “no opinion,” or equivalent

---

<sup>94</sup> *Dynata Panel Book*. Available at [www.dynata.com/panel-book-form](http://www.dynata.com/panel-book-form).

<sup>95</sup> “Traditionally, scientists adopt the 95% level of confidence, which means that if 100 samples of the same size were drawn, the confidence interval expected for at least 95 of the samples would be expected to include the true population value.” See Diamond, S. (2011). “Reference Guide On Survey Research,” in Reference Manual on Scientific Evidence. Federal Judicial Center/National Academy of Sciences, p. 381.

answer option wherever appropriate throughout the survey to minimize guessing or forcing respondents to select an answer where they may not have a strong opinion.

152. It is common in consumer survey research for the researcher to employ various types of randomization of questions and answer options across respondents. Randomization is an important tool that researchers use to minimize the potential for order bias (i.e., order effects) to impact the study's results. Order bias refers to a respondent's tendency to select the first answer in a given list of answer options regardless of the question content<sup>96</sup> or answer the first question in a series of questions differently than later questions.<sup>97</sup> In this study, randomization was used wherever possible to minimize the potential for order bias.
153. To ensure the integrity of the data, I sought to identify "speeders" for potential removal from the sample. Respondents who complete a survey too quickly may introduce respondent-related error into the survey data. Respondents were to be flagged if they completed the survey in less than one-third of the median completion time across all respondents in the sample. One respondent was removed from the sample based on this criterion (provided at Exhibit 5).
154. Consistent with standard survey methodologies and practices, the screening portion of the questionnaire also employed security questions, including a CAPTCHA question to prevent bots and other automated respondents from participating in the study. Respondents who did not pass the security measures were not permitted to complete the survey.
155. The study was conducted under "double blind" conditions—neither the panel provider nor the survey participants knew the purpose of the study or the sponsoring party. Double blind

---

<sup>96</sup> Visser, P. S., Krosnick, J. A., & Lavrakas, P. J. (2000). Survey research. In H. T. Reis & C. M. Judd (Eds.), *Handbook of Research Methods in Social and Personality Psychology*. Cambridge University Press, p. 240.

<sup>97</sup> See Diamond, S. (2011). "Reference Guide On Survey Research," in Reference Manual on Scientific Evidence. Federal Judicial Center/National Academy of Sciences, p. 396: "To control for order effects, the order of the questions and the order of the response choices in a survey should be rotated, so that, for example, one-third of the respondents have Product A listed first, one-third of the respondents have Product B listed first, and one-third of the respondents have Product C listed first. If the three different orders are distributed randomly among respondents, no response alternative will have an inflated chance of being selected because of its position, and the average of the three will provide a reasonable estimate of response level."

research is designed to prevent external or circumstantial bias from impacting the survey process and results.

### **Questionnaire**

156. The survey questionnaire consisted of two parts: a screening portion, which confirmed that respondents met the qualification criteria for participation in the study; and the main questionnaire, which administered the key measures of interest. The language and mechanics of the screener and main questionnaire are provided in summary below; screenshots of the questionnaire as it was viewed by respondents are provided at Exhibit 3.
157. The screener opened with a standard survey research statement that conveyed relevant information about duration, privacy issues, etc., and instructed respondents not to guess if they did not know the answer to a question but, instead, to use the “Don’t know” option that was provided when appropriate. Only respondents who indicated that they understood the instructions were allowed to continue with the survey.
158. The next question asked respondents to provide their age. Only respondents aged 18 and older were permitted to continue with the survey:

Which of the following age brackets contains your age on your last birthday?

m Under 18

m 18 - 30

m 31 - 40

m 41 - 50

m 51 - 60

m 61 - 70

m 71 or older

159. On the next screen, respondents were asked to indicate the state in which they reside. This question was for demographic information purposes only and was not used to filter out any respondents:

In which U.S. state do you currently reside?

Alabama ▼

160. Respondents were next asked to indicate their gender. This question was for demographic information purposes only and was not used to filter out any respondents:

What is your gender?

m Male

m Female

m Prefer to self-identify: \_\_\_\_\_

m Prefer not to answer

161. The next screening question was a CAPTCHA-type security measure; it was included to confirm that respondents were devoting appropriate attention to their responses and to prevent bots and other automated respondents from participating in the study. Only respondents who answered the question correctly were permitted to continue with the survey.

162. Respondents were next asked about the types of Internet browsers they have used during the last five years:

Which of the following Internet web browsers, if any, have you used in the last five years? Please select all that apply.

- ☐ Safari
- ☐ Chrome
- ☐ Edge / Internet Explorer
- ☐ Other
- ☐ Don't know

163. Because Plaintiffs seek to represent users of private browsing mode in Chrome, Safari, and Edge/Internet Explorer, only respondents who indicated that they had used one or more of those browsers during the Class Period were permitted to continue with the survey. All other respondents were terminated.

164. Respondents were next asked about their use of private browsing mode in each of the relevant browsers (i.e., Chrome, Safari, and Edge/Internet Explorer). This question employed dynamic piping: respondents were only asked about their private browsing behaviors for the browsers they indicated they had used in the previous question. Respondents were asked:

Some Internet web browsers offer a private browsing mode. Which of the following types of private browsing, if any, have you used in the last five years? Please select all that apply.

- ☐ Private browsing mode in Chrome ("Incognito")
- ☐ Private browsing mode in Edge / Internet Explorer ("InPrivate")
- ☐ Private browsing mode in Safari ("Private Browsing Mode")
- ☐ None of these

165. Again, because Plaintiffs seek to represent users of private browsing mode in Chrome, Safari, and Edge/Internet Explorer, only respondents who indicated that they had used private browsing mode in one or more of those browsers during the Class Period were permitted to continue with the survey. All other respondents were terminated.

166. Respondents who indicated that they had used private browsing mode in Chrome, Safari, and/or Edge/Internet Explorer during the last five years were confirmed to be potential Class Members and deemed qualified to participate in the study. These respondents advanced to the main portion of the questionnaire.

167. The main portion of the questionnaire began with the following instruction intended to reduce guessing among respondents:

For the remainder of this survey, if you do not know or do not have an opinion about any of the questions, please select the "don't know / no opinion" answer option. Please do not guess at any of your answers and please do not use the Internet or any other sources to inform your answers.

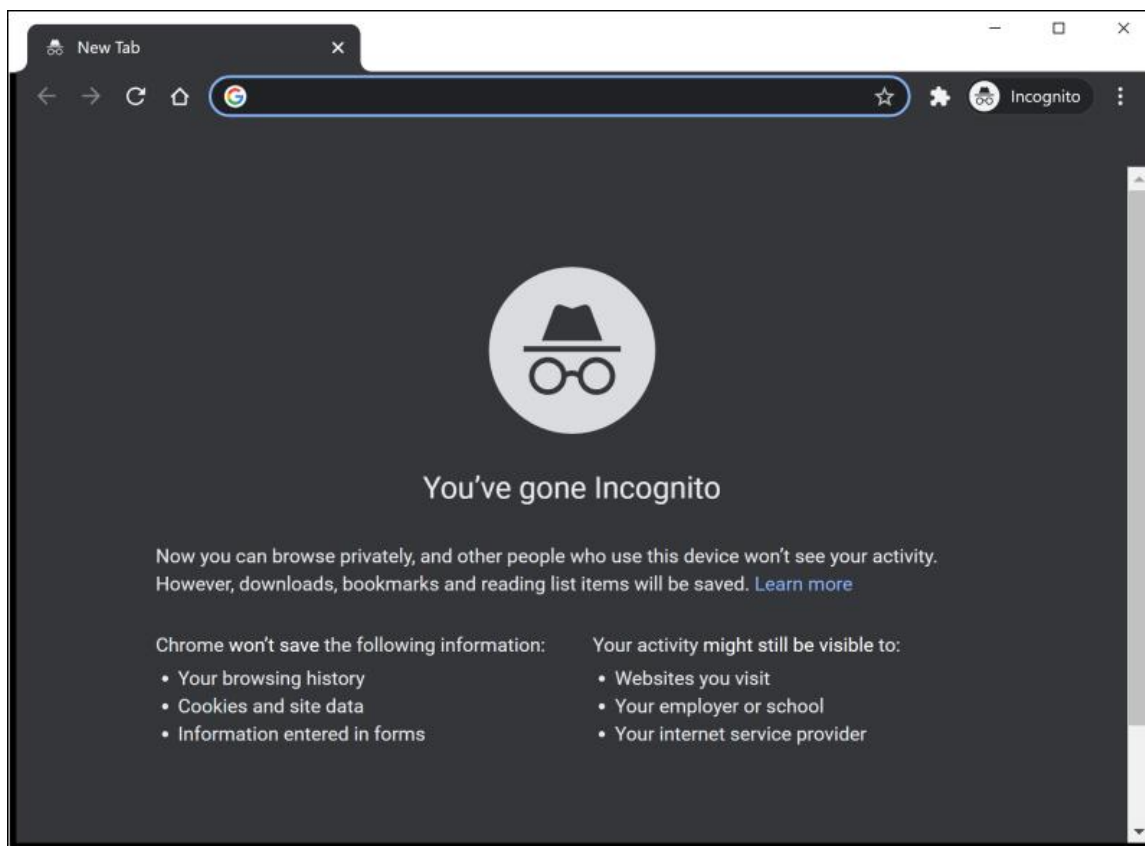
168. Respondents were next exposed to one PBM splash screen for Chrome, Safari, or Edge/Internet explorer. For this study, I used the same (unmodified) Chrome Incognito splash screen that was used in the Amir Studies. It is my understanding that this version of the Chrome splash screen was in use for the majority of the Class Period. I also used the same Safari splash screen that was used in the Amir Studies. Because the Amir Studies did not address any issue related to Edge/Internet Explorer, there was no Edge splash screen stimulus in Professor Amir's production. I therefore used a current<sup>98</sup> and unmodified Edge splash screen image.

---

<sup>98</sup> Accessed 4/28/2022.

169. Assignment to the study stimulus was determined as follows: any respondent who indicated using Chrome (singularly or in combination with Safari and/or Edge/Internet Explorer) saw the Chrome splash screen; any respondent who indicated using only Safari saw the Safari splash screen; any respondent who indicated using only Edge/Internet Explorer saw the Edge splash screen; and any respondent who indicated using both Safari and Edge/Internet Explorer (but not Chrome) were randomly assigned to see either the Safari or the Edge/Internet Explorer splash screen. Respondents were provided with an instruction to view the stimulus as they would when opening a new PBM window<sup>99</sup> (Chrome stimulus presentation used here for demonstration purposes; All study stimuli available at Exhibit 3):

Shown below is the screen that displays when a new Chrome Incognito window is opened. Please review it as you normally would when opening a new Chrome Incognito window. You can view the image for as long as you would like. You may click on the image for an enlarged view.



<sup>99</sup> It is my understanding that this version of the Chrome splash screen was in use for the majority of the Class Period.

170. To accurately replicate the ways in which users interact with the PBM splash screen when starting a new private browsing session, respondents were not required to view the splash screen for any specific amount of time. Respondents were instructed to click the “Next” button at the bottom of the page when they were ready to continue.

171. The next sequence of questions constitutes the key measures of interest of the study. These questions were designed to measure the proportion of the sample that believes they have consented to Google’s PBM data collection and storage practices (without addressing the issue of Google’s use of this data). Respondents were first asked:

Please think of the time(s) that you have used private browsing mode to browse the Internet in the last five years.

Which of the following best reflects your understanding:

m Google **collects and saves** my Internet browsing activity when I browse the Internet in private browsing mode

m Google **does not collect and save** my Internet browsing activity when I browse the Internet in private browsing mode

m Don't know / No opinion

172. Respondents who indicated a belief that Google “does not collect and save” Internet browsing activity when users browse the Internet in private browsing mode were considered misinformed about Google’s PBM data collection and storage practices based on the allegations in the Complaint and skipped to the data integrity question (discussed below). Respondents who indicated a belief that Google “collects and saves” Internet browsing activity when users browse the Internet in private browsing mode or selected the “don’t know” option advanced to the next question.

173. The next question was designed to measure the extent to which remaining respondents believed they had provided Google with consent to collect information about their Internet browsing activity when in PBM. Respondents were asked:



Please think of the time(s) that you have used private browsing mode to browse the Internet in the last five years.

Which of the following best reflects your beliefs about the level of consent that you provide Google to collect information about your Internet browsing activity when in private browsing mode?

☐ I believe that when I am in private browsing mode, **I have given consent** for Google to collect and save information about my Internet browsing activity

☐ I believe that when I am in private browsing mode, **I have not given consent** for Google to collect and save information about my Internet browsing activity

☐ Don't know / No opinion

174. Respondents who indicated a belief that they “have not given consent” for Google to collect and save information about their Internet browsing activity when in PBM were considered misinformed about Google’s PBM data collection and storage practices based on the allegations in the Complaint and skipped to the data integrity question. Respondents who indicated a belief that they “have given consent” for Google to collect and save information about their Internet browsing activity when in PBM or selected the “don’t know” option advanced to the next question.

175. The next question was designed to collect information about the circumstances under which remaining respondents believed they had provided Google with consent to collect and save information about their Internet browsing activity when in PBM. Respondents were asked:

Which of the following best reflects your opinion?

I believe that when I am in private browsing mode, I have given consent for Google to collect and save information about my Internet browsing activity (please select all that apply):

- ☐ When I am visiting a **Google website**
- ☐ When I am visiting a **non-Google website**
- ☐ Don't know

176. Respondents who indicated a belief that they had given consent for Google to collect and save information about their Internet browsing activity when in PBM *only* when visiting a Google website were considered misinformed about Google’s PBM data collection and storage practices based on the allegations in the Complaint and skipped to the data integrity question. Respondents who indicated a belief that they had given consent for Google to collect and save information about their Internet browsing activity when in PBM when

visiting a non-Google website or selected the “don’t know” option advanced to the next question.

177. Remaining respondents were next asked a question to determine whether they had a Google account during the Class Period. Respondents were asked:

If you know, which of the following types of accounts have you had at any time during the last five years? Please select all that apply.

- ☐ Google account (e.g., Gmail, Google Docs, Google Drive, Google Photos)
- ☐ Microsoft account (e.g., OneDrive, Microsoft Teams, OneNote)
- ☐ Apple account (e.g., iCloud, Apple Pay, Apple Music)
- ☐ None of these

178. Respondents who indicated that they had a Google account during the Class Period were asked a question to determine their beliefs regarding whether they had given Google consent to collect and save information about their Internet browsing activity when in PBM and signed out of their Google account. Respondents were asked:

Which of the following best reflects your opinion?

I believe that when I am in private browsing mode, I have given consent for Google to collect and save information about my Internet browsing activity (please select all that apply):

- ☐ When I am **signed in** to my Google account
- ☐ When I am **signed out** of my Google account
- ☐ Don't know

179. Respondents who indicated a belief that they had given consent for Google to collect and save information about their Internet browsing activity when in PBM *only* when signed in to their Google account were considered misinformed about Google’s PBM data collection and storage practices based on the allegations in the Complaint and skipped to the data integrity question. Respondents who indicated a belief that they had given consent for Google to collect and save information about their Internet browsing activity when in PBM when signed out of their Google account or selected the “don’t know” option advanced to the next question.

180. The final question in the sequence of key measures was designed to collect beliefs of remaining respondents with respect to the types of information they believe Google collects about their Internet browsing behavior when in PBM. Respondents were asked:

Please think of the time(s) that you have used private browsing mode to browse the Internet in the last five years.

Would you or would you not expect Google to collect and save each of the following types of information about your Internet browsing behavior during your private browsing mode session?

	Yes, Google would collect and save	No, Google would not collect and save	Don't know
URL information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
HTTP information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cookies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your browsing activity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your IP address	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your user agent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your geolocation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your unique user ID	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

181. All respondents were next required to answer a data integrity question (i.e., attention filter) designed to ensure that they were taking the questionnaire seriously and devoting sufficient attention to reading and understanding the questionnaire. Respondents were asked:

Please select "Green" from the list below.

- m Red
- m Green
- m Blue
- m Yellow

182. Only respondents who selected “Green” were permitted to continue with the survey. All other respondents were terminated.

183. The main questionnaire concluded with additional standard demographic questions regarding education and household income. The full questionnaire is provided at Exhibit 3.

### **Sample characteristics**

184. The sample for this study is nationally representative, providing a robust, projectable overview of the perceptions and expectations of prospective Class Members. Demographic characteristics for the study participants are shown in Table 5 below.

Table 5. Sample characteristics - demographics

	<b>% Respondents</b> (n=1,052)
<b>Age</b>	
18 - 30	18.4
31 - 40	22.6
41 - 50	20.0
51 - 60	13.2
61 - 70	15.1
71 or older	10.6
<b>Education</b>	
Less than high school	2.2
High school graduate	21.9
Some college	22.6
2-year degree	12.3
4-year degree	26.2
Master's / Professional degree	12.6
Doctorate	2.2
<b>Household income</b>	
Under \$35,000	23.7
\$35,000 - \$49,999	17.3
\$50,000 - \$74,999	18.3
\$75,000 - \$99,999	15.7
\$100,000 - \$124,999	9.3
\$125,000 - \$149,999	6.3
\$150,000 or more	7.6
I prefer not to answer	1.8
<b>Region</b>	
Northeast	20.1
South	40.1
Midwest	20.1
West	19.8
<b>Gender</b>	
Male	50.0
Female	49.9
Prefer to self-identify	0.1
Prefer not to answer	0.0

**Findings**

185. The findings of this study provide empirical evidence that nearly all potential Class Members—93.1 percent—are misinformed about Google’s PBM data collection and storage practices based on the allegations in the Complaint.<sup>100</sup> In contrast, fewer than one-in-ten

<sup>100</sup> Google asserts that “Numerous third-party articles have explained that Google receives the at-issue data while users are in Incognito mode.” (see Defendant’s Supplemental Objections and Responses to Plaintiffs’ Interrogatories Set 9 (Nos. 40), p. 11). A review of these articles shows that they were all published prior to

respondents—6.9 percent—provided responses indicating that they believed they understood and consented to Google’s PBM data collection and storage practices (or do not know), without addressing how Google uses PBM data. Table 6 below provides a summary of the key study findings.

*Table 6. Consumer understanding of Google PBM data collection and storage practices*

<i>Base: All respondents (n=1,052)</i>	<b>% Respondents</b>
<b><i>Misinformed about Google PBM data collection and storage practices</i></b>	
Google does not collect and save my Internet browsing activity in private browsing mode	54.8
I have not given consent to Google to collect and save my Internet browsing activity when I browse the Internet in PBM	20.2
I have given consent to Google to collect and save my Internet browsing activity in PBM only when visiting a Google website	11.8
I have given consent to Google to collect and save my Internet browsing activity in PBM only when signed in to my Google account	3.6
Indicated a belief that Google would not collect and save at least one type of data displayed in the matrix table	2.8
<b>Total misinformed about Google PBM data collection and storage practices</b>	<b>93.1</b>
<b><i>Informed or don’t know</i></b>	<b>6.9</b>
<b><i>Total</i></b>	<b>100.0</b>

186. As shown in Table 6, over half of PBM users—54.8 percent—indicated a belief that Google does not collect and save their Internet browsing activity at all when browsing in PBM, before even asking about visiting non-Google websites while not signed in to any Google account.

187. Additionally, of the entire sample, one-in-five respondents—20.2 percent—indicated a belief that they have not given consent to Google to collect and save their Internet browsing activity when they browse the Internet in PBM. An additional 11.8 percent of respondents believed that they had given consent to Google to collect their Internet browsing activity when using PBM only when visiting a Google website, and 3.6 percent believed that they had given

---

the start of the Keegan Study, therefore all information contained in those articles are accounted for in my results.

consent to Google to collect their Internet browsing activity when using PBM only when signed in to their Google account.

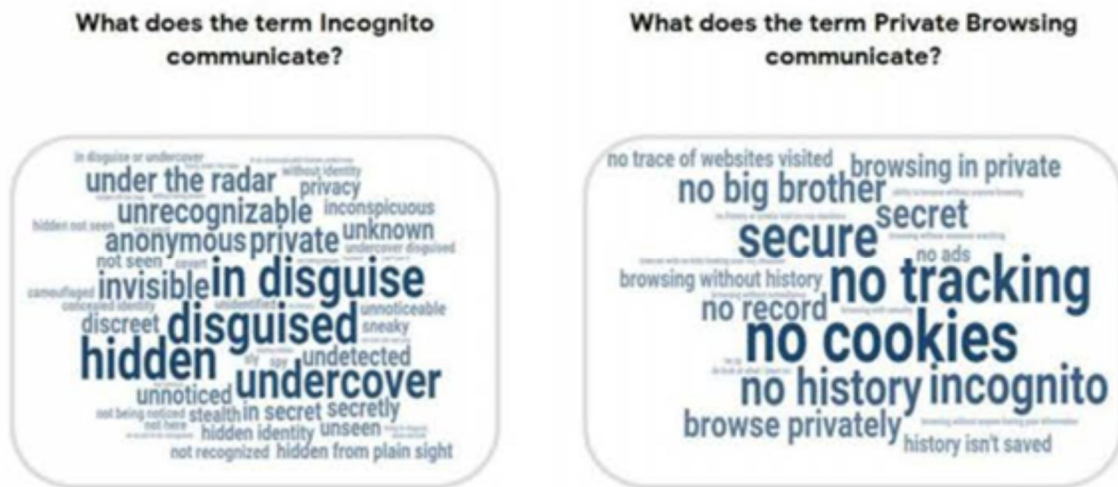
188. An additional 2.8 percent of respondents were misinformed about the types of personal information that Google collects when users browse in PBM.
189. In total, 93.1 percent of the sample were misinformed about Google's PBM data collection and storage practices based on the allegations in the Complaint.
190. Overall, just 6.9 percent of study respondents provided answers indicating they believed they had consented to Google's PBM data collection and storage practices or consistently demonstrated an awareness of what Google's PBM data collection and storage practices are (as alleged in the Complaint) or didn't know across all measures.
191. This study provides empirical evidence that Class Members are not aware of or do not believe they have consented to Google's PBM data collection and storage practices.
192. Because the study accurately replicated the marketplace conditions under which typical PBM users encounter the Chrome, Safari, and Edge/Internet Explorer splash pages and employed objective, non-leading questions, the study data provides a reliable basis for projection to the larger universe of Class Members.

## **VI. Analysis of Google Internal Documents**

193. Another indicator that the Amir Studies do not yield any valid or reliable evidence on the issues that are relevant to this case is the fact that the findings of the Amir Studies and opinions in the Amir Report do not align with—and, in fact, stand in contrast to—a body of research and other evidence produced by Google in this matter, which provides further evidence in support of the existence of common misconceptions about Google's PBM data collection and storage practices.
194. For example, a Google study of [REDACTED] Incognito and other PBM users showed that consumers largely overestimate the privacy protections offered by Chrome Incognito with what Google characterized as “common misconceptions”:

Participants overestimate private mode protections. There are several common misconceptions about private mode, including that it prevents all external parties from accessing user data and search history...protects against tracking and ad targeting, gives anonymity, obscures location, hides browsing activity from Google.<sup>101</sup>

195. This Google study also contains the following word map of concepts often cited by participants when asked their opinions about what the terms “Incognito” and “Private Browsing” communicate:<sup>102</sup>



196. As shown above, the concepts most often cited by respondents (large, bold lettering) center on issues related to anonymity and a lack of data collection, tracking, etc. This shows that users have an expectation of privacy and of not being tracked when engaging in private browsing, which is consistent with my findings.

197. Google’s research also shows that “most users are not aware of session-based tracking”<sup>103</sup> and that a “majority of users expect no session-based tracking.”<sup>104</sup> Users also expressed that they didn’t want Google to collect data in Incognito, especially data tied to their identity.<sup>105</sup>

<sup>101</sup> GOOG-BRWN-00042403.

<sup>102</sup> GOOG-BRWN-00042412.

<sup>103</sup> GOOG-BRWN-00042404.

<sup>104</sup> GOOG-BRWN-00042404.

<sup>105</sup> GOOG-BRWN-00042408.

Google's research notes that "Given that participants overestimate private browsing mode protections, participants are surprised and feel misled when made aware of private mode vulnerabilities."<sup>106</sup>

198. These Google documents recognize a lack of awareness among PBM users extends both to use of Incognito even when logged in to a Google account. One Google study showed that [REDACTED] of Incognito users believed that Google would not remember their browsing history even if they use Incognito when logged in to Gmail or another Google account.<sup>107</sup> Based on this, the study concluded that most Chrome users do not understand what is and is not saved when logging into an account in Incognito, even when they are experienced at using it."<sup>108</sup>

199. Google's documents also demonstrate an awareness from internal research that Google's disclosures are often disregarded or outright ignored by users. Noting that "participants often click through or ignore disclosures,"<sup>109</sup> Google's research shows that "most users don't properly read disclosure text yet in-context reminders about misconceptions can be confusing and misleading."<sup>110</sup>

200. Additionally, the Chrome Incognito splash screen, with its disguised Incognito icon, is a powerful signal that communicates a sense of privacy and anonymity to users. Google's research confirms that this is misleading:

...Many users are confused about the privacy properties of Incognito, tying our icon and the name 'Incognito' to feelings of 'stealth' or being 'in hiding.' But Incognito (and private browsing mode broadly) only prevents users from saving information on their device. Private browsing does not make users invisible to external services, such as the accounts they log into.<sup>111</sup>

201. A wealth of internal Google communications and additional studies, summarized in Exhibit 8 to this report, support the Google research findings presented here. For example, one Google

---

<sup>106</sup> GOOG-BRWN-00042409.

<sup>107</sup> GOOG-BRWN-00042350.

<sup>108</sup> GOOG-BRWN-00042350.

<sup>109</sup> GOOG-BRWN-00042409.

<sup>110</sup> GOOG-BRWN-00042418.

<sup>111</sup> GOOG-BRWN-00042340.



employee noted that “The spy imagery is absolutely NOT what we want to keep portraying. It’s unfortunate that we already have it. Incognito does NOT support the kinds of guarantees that people imagine for a ‘spy mode.’”<sup>112</sup> Another communication stated, “Users have misconceptions about Incognito and often overestimate the protections available.”<sup>113</sup>

202. The range of relevant information outlined herein was available to Professor Amir as well, and yet the Amir Studies did not directly test concepts related to Class Members’ beliefs and expectations regarding Google’s PBM data collection and storage practices. Rather, the Amir Studies adopted a tangential approach focused on (a) ill-defined “entities” and oversimplified types of information that might be “received” when users engage in private browsing, and (b) irrelevant likelihood of use measures. The Amir Studies’ heavy focus on forced exposure to Google and other private browsing disclosures obscures the relevant research issue in this matter—i.e., the perceptions and expectations of potential Class Members regarding Google’s PBM data collection and storage practices, and specifically, the extent to which Google collects and saves the user’s personal information when using PBM.

203. As described herein, the Keegan Study addressed this issue directly and showed that, consistent with Google’s internal research, nearly all Class Members are misinformed about Google’s PBM data collection and storage practices based on the allegations in the Complaint.

## VII. Conclusions

204. As described in detail throughout this report, none of the three Amir Studies provide valid or reliable evidence regarding the perceptions, expectations, beliefs, or behaviors of any reasonable Class Member with respect to Google’s PBM data collection and storage practices. As such, the Amir Studies provide no valid or reliable support for Professor Amir’s stated opinions with respect to any Class Members.

205. The Keegan Study, which was designed to correct many of the deficiencies and limitations of the Amir Studies, provides empirical evidence that a reasonable member of either of the two Classes would be and the vast majority of all Class Members are misinformed about the

---

<sup>112</sup> GOOG-BRWN-00812091.

<sup>113</sup> GOOG-CABR-04668451.

Google PBM data collection and storage practices alleged in the Complaint and at issue in this lawsuit.

I reserve the right to supplement and revise this report and the opinions expressed herein based on the availability of new information.

A handwritten signature in black ink, reading "Mark Keegan", written over a horizontal line.

Mark Keegan

May 20, 2022

Date

**Exhibit 1—Mark Keegan C.V.**



**KEEGAN & DONATO**  
CONSULTING, LLC

31 Purchase Street, Ste. 3-4  
Rye, New York 10580  
914.967.9421  
www.keegandonato.com

**Mark T. Keegan, Esq.**

**Partner, Keegan & Donato Consulting, LLC**

**Education**

- § Principles of Market Research Program, University of Georgia (graduated 2021)
  - Post-graduate program for industry professionals covering all aspects of the market research process
  - Coursework based on the Market Research Core Body of Knowledge (MRCBOK), a compilation of the underlying principles and essential skills that comprise the market research process developed by Market Research Institute International (MRII)
  - Certification conferred upon participants who demonstrate mastery of concepts presented in 284 detailed module studies across 13 core areas of market research
  - Endorsed by all major market research and insights industry associations, including ESOMAR and the Insights Association
- § Professional Certified Marketer (PCM), American Marketing Association (2015 – present)
  - AMA certification for individuals who have demonstrated a mastery of comprehensive and core marketing knowledge and principles
  - Designation conferred only upon successful completion of rigorous testing spanning full range of marketing principles and concepts
  - Ongoing professional development and education credits required on annual basis
  - PCM recipients must have demonstrated professional experience in the field of marketing
- § Juris Doctor, Brooklyn Law School (graduated 1995)
- § Bachelor of Arts, History, Pace University (graduated 1990)
- § MBA Coursework, Pace University, Lubin School of Business (1990 – 1991)
- § Corporate Finance Program, Harvard University (coursework)

### **Professional Memberships**

- § Admitted to the Bar in the states of New York and Connecticut
- § Member, ESOMAR (World Association of Opinion and Marketing Research Professionals)
- § Member, International Trademark Association (INTA)
- § Member, American Marketing Association (AMA)
- § Member, American Association for Public Opinion Research (AAPOR)
- § Member, Association for Consumer Research (ACR)
- § Registered Representative, National Association of Securities Dealers (Series 7, expired)

### **Current Employment**

- § Keegan & Donato Consulting, LLC, Litigation Consultant, Founding Partner (7/2011 – present)

### **Consumer Research Experience**

- § Designed and executed over 1,000 consumer research studies reaching more than 250,000 respondents for corporate and litigation clients over the course of two-decade career
- § Focus on trademark and marketing research with principal areas of study including consumer confusion, trade dress, dilution, secondary meaning, genericness, false advertising, consumer perception, consumer understanding, and other consumer research issues
- § Represented a mix of both plaintiffs and defendants in litigation matters spanning a broad range of products, services, and industries
- § Submitted survey research expert reports in relevant venues including federal courts, state courts, at arbitration, to the National Advertising Division of the Council of Better Business Bureaus, and to the Trademark Trial and Appeal Board
- § Founder and owner of two successful marketing and consumer research consulting firms
- § Regularly testify to consumer behavior research, findings, and related issues at trials, depositions, hearings, and other proceedings

§ Qualified to testify as an expert in the field of consumer survey research at federal court trials:

- *BuzzBallz, LLC v. Jem Beverage Co.*, U.S. District Court (Central District of California), the Honorable William D. Keller presiding
- *Christopher Lewert v. Boiron, Inc.*, U.S. District Court (Central District of California), the Honorable André Birotte, Jr. presiding
- *Coty Inc., et al. v. Excell Brands LLC*, U.S. District Court (Southern District of New York), the Honorable Jesse M. Furman presiding
- *Bodum U.S.A., Inc. v. A Top New Casting, Inc.*, U.S. District Court, Northern District of Illinois, the Honorable Matthew F. Kennelly presiding

§ Qualified as a survey expert by numerous federal court judges (pre-trial)

§ Develop and execute consumer research studies using industry-accepted methodologies, cutting-edge technologies, and industry-leading consumer panel partners

#### **Marketing and Other Relevant Experience**

§ Served as a marketing consultant to private clients and have advised on a wide range of issues including product development and rollout, advertising, consumer feedback and intelligence, the product life-cycle, and other issues concerning marketing and marketing research

§ Formulated winning brand positioning strategies as a branding expert for some of the best-known consumer brands and services including General Electric (GE), Nike, Pepsi, Subaru, AOL, Excite, NBC, and others

§ Analyzed and evaluated comprehensive marketing campaigns for a broad range of corporate clients to determine their impact on consumers

§ Evaluated all components of integrated marketing communications including advertising, public relations, packaging, sales promotions, and point of sale materials, among others

§ Developed testimony on marketing messages and their intended influence on consumer understanding and behavior

**Previous Employment**

## § Keegan &amp; Company LLC, Founding Partner (9/2001 – 12/2015)

Designed and executed consumer research studies, conducted complex litigation consulting, and developed marketing and economic analyses for clients across a range of industries

## § Information Markets Corp, Program Manager (2000 – 2001)

Managed enterprise-wide marketing and product development. Developed use cases and conducted consumer market research. Coordinated with multiple partners including AOL, Excite, and NBC.

## § Affiliation Networks, Inc., Project Manager (1999 – 2000)

Produced online advertising solutions for Fortune 500 clients. Coordinated creative team of account managers, designers, programmers and copywriters.

## § UpTick Technologies, Marketing Consultant (1999)

Managed the creation of innovative marketing products for large brokerage software provider

## § Cosmos Internet Solutions, Marketing Consultant (1998 – 1999)

Developed marketing strategy for business ISP and hosting provider as well as Web site marketing and development for clients

## § FactSet Research Systems, Product Development (1996 – 1998)

Formulated product and communications strategies for leading integrated financial and economic database provider

## § Warren Keegan Associates, Inc., Marketing Consultant (1992 – 1996)

Marketing consultant to clients across a range of industries. Edited and contributed content to marketing textbooks and other academic marketing publications.

## § BMW of North America, Inc., Graduate Appointment (1991)

Reviewed, analyzed, and cataloged broad-based market research on consumer preferences and attitudes in the automobile industry

**Submitted Surveys Excluded by Courts\***

- § *Kudos, Inc. v. Kudoboard, LLC, et al.* (2021). This Squirt-style survey was designed to test for a likelihood of confusion between two competing brands of employee recognition software among users and likely purchasers of this type of software. The Court disagreed with the survey universe, opining that a narrower population definition should have been employed. A rebuttal report that I submitted in this matter was accepted by the Court.
- § *The Episcopal Church, et al. v. The Right Reverend Mark J. Lawrence, et al.* (2019). In this Teflon-style survey, I interviewed Episcopalians regarding the potential genericness of the mark THE EPISCOPAL CHURCH. The Court disagreed with the survey universe, opining that the population definition should have included non-Episcopalians.
- § *Warner Brothers Entertainment, Inc., et al. v. The Global Asylum, Inc.* (2012). A deficiency in the pleadings (the client's failure to submit my resume among other credentials) led to the court excluding this survey at a preliminary injunction hearing. I did not testify in this matter.

**Lectures, Presentations & Publications**

- § *Squirt vs. Eveready: Battle of the Titans*, 9<sup>th</sup> Annual Intellectual Property Law Symposium, hosted by The Florida Bar Continuing Legal Education Committee and Business Law Section, April 12-13, 2018. CLE-accredited presentation.
- § *Panel Power: Online Panel Sampling for Litigation Surveys*, 8<sup>th</sup> Annual Intellectual Property Law Symposium, hosted by The Florida Bar Continuing Legal Education Committee and Business Law Section, March 30-31, 2017. CLE-accredited presentation.
- § *Evaluating a Brand's Equity in a Nascent Market*, ESOMAR World Research, The EUREKA's Project - Success Stories of Market Research, 2016.
- § *Consumer Survey Research for Litigation: With Great Data Comes Great Power*. Presentation before the Pennsylvania Bar Association, Intellectual Property Law Group, 12/8/2014.

---

\* Lifetime. Court opinions available upon request.



### **Continuing Education**

- § *Online Sample Fraud: Causes, Costs & Cures*, Insights Association Webinar, 2/11/2022.
- § *Quantifying Unjust Enrichment*, Fox Forensic Accounting, 10/6/2021.
- § *Questionnaire Design Best Practices*, ESOMAR/University of Georgia Webinar, 5/19/2021.
- § *Making Online Samples More Representative*, ESOMAR Webinar, 3/17/2021.
- § *Intelligence 360: Solicited + Unsolicited Customer Opinion*, ESOMAR Webinar, 2/17/2021.
- § *The Future of Online Polling After 2020*, ESOMAR Webinar, 12/16/2020.
- § *The Opportunity for UX Research*, ESOMAR/University of Georgia Webinar, 12/8/2020.
- § *BigSurv20: Big Data Meets Survey Science*, Online Conference, November/December 2020.
- § *International Trademark Association (INTA), 141st Annual Meeting (2019)*, Attendee, May 2019.

### **Contact Information**

Keegan & Donato Consulting, LLC  
31 Purchase Street, Ste. 3-4  
Rye, NY 10580  
(914) 967-9421  
mark@keegandonato.com



**KEEGAN & DONATO**  
CONSULTING, LLC

31 Purchase Street, Ste. 3-4  
Rye, New York 10580  
914.967.9421  
www.keegandonato.com

## Mark Keegan Testimony List (Past Four Years)

### Depositions

Case Caption	Court	Client
BillFloat Inc., d/b/a SmartBiz Loans v. Collins Cash Inc., d/b/a Smart Business Funding, et al.	United States District Court, Northern District of California	Defendants
Kenco Bucket Trucks LLC v. Versabucket LLC, et al.	District Court, Harris County, Texas, 113 <sup>th</sup> Judicial District	Defendants
EBIN New York, Inc. v. SIC Enterprise, Inc., et al.	United States District Court, Eastern District of New York	Plaintiff
Kudos, Inc. v. Kudoboard, LLC, et al.	United States District Court, Northern District of California	Plaintiff
Master Inspector Certification Board, Inc. v. Examination Board of Professional Home Inspectors, Inc.	United States Patent and Trademark Office, Trademark Trial and Appeal Board	Plaintiff (Petitioner)
Solid 21 Inc. v. Richemont North America, Inc. et al.	United States District Court, Southern District of New York	Defendants
Watching Time, LLC v. International Watchman, Inc.	United States Patent and Trademark Office, Trademark Trial and Appeal Board	Plaintiff (Petitioner)
Diamond Resorts U.S. Collection Development, LLC, et al. v. Newton Group Transfers, LLC, et al.	United States District Court, Southern District of Florida, West Palm Beach Division	Defendants
Fair Isaac Corporation v. Fido Alliance, Inc.	United States Patent and Trademark Office, Trademark Trial and Appeal Board	Defendant (Applicant)
Solid 21, Inc. v. Breitling U.S.A. Inc., et al.	United States District Court, District of Connecticut	Defendants
Juul Labs, Inc. v. Eonsmoke, LLC d/b/a 4X PODS, et al.	United States District Court, District of New Jersey	Defendants
Restoration Hardware, Inc., et al., v. Bungalow Home, LLC	United States District Court, Southern District of Ohio, Western Division	Plaintiffs

KEEGAN\_EXHIBITS\_8



# KEEGAN & DONATO CONSULTING, LLC

31 Purchase Street, Ste. 3-4  
Rye, New York 10580  
914.967.9421  
www.keegandonato.com

Case Caption	Court	Client
United States of America ex. rel., Yoash Gohil v. Sanofi U.S. Services Inc., et al.	U.S. District Court, Eastern District of Pennsylvania	Defendants
Alo, LLC v. Acadia Malibu, Inc., d/b/a Alo House Recovery Centers, et al.	U.S. District Court, Central District of California	Plaintiff
Farjad Fani, et al. v. Shartsis Friese LLP, et al.	JAMS Arbitration, JAMS Reference No. 1100104777	Claimants
Solid 21, Inc. v. Ulysse Nardin USA Inc., et al.	U.S. District Court, Southern District of Florida	Defendants
The Shoppes at River Station, LLC v. College Park Retail Investors, LLC	Superior Court of Fulton County, State of Georgia	Plaintiff
Spartan Chemical Company, Inc. v. Ecolab, Inc.	U.S. District Court, Northern District of Ohio, Western Division	Plaintiff
Allergan USA, Inc. v. Imprimis Pharmaceuticals, Inc.	U.S. District Court, Central District of California, Southern Division	Defendant
The Episcopal Church, et al. v. The Right Reverend Mark J. Lawrence, et al.	U.S. District Court, District of South Carolina, Charleston Division	Plaintiffs
Spangler Candy Company v. Tootsie Roll Industries, LLC	U.S. District Court, Northern District of Ohio, Western Division - Toledo	Plaintiff
FCOA LLC v. Foremost Title & Escrow Services, LLC	U.S. District Court, Southern District of Florida	Defendant
Dentsply International Inc. v. Dental Brands for Less LLC d/b/a Dental Wholesale Direct	U.S. District Court, Southern District of New York	Plaintiff
eMove, Inc. and u-Haul International, Inc. v. Hire A Helper, LLC, et al.	U.S. District Court, Southern District of California	Defendants
J-B Weld Company, LLC v. The Gorilla Glue Company	U.S. District Court, Northern District of Georgia	Defendant
Gulfstream Aerospace Corp. v. Gulfstream Unsinkable Boats, LLC	U.S.P.T.O. Trademark Trial and Appeal Board	Defendant
Lokai Holdings, LLC v. Twin Tiger USA LLC	U.S. District Court, Southern District of New York	Plaintiff
Michael Kors, LLC v. Chunma, USA, Inc., et al.	U.S. District Court, Central District of California	Defendant

KEEGAN\_EXHIBITS\_9



**KEEGAN & DONATO**  
**CONSULTING, LLC**

31 Purchase Street, Ste. 3-4  
Rye, New York 10580  
914.967.9421  
[www.keegandonato.com](http://www.keegandonato.com)

Case Caption	Court	Client
Mars, Inc. et al. v. The J.M. Smucker Company, et al.	U.S. District Court, Eastern District of Virginia	Plaintiffs
Bodum U.S.A., Inc. v. A Top New Casting, Inc.	U.S. District Court, Northern District of Illinois, Eastern Division	Defendant



# KEEGAN & DONATO CONSULTING, LLC

31 Purchase Street, Ste. 3-4  
Rye, New York 10580  
914.967.9421  
[www.keegandonato.com](http://www.keegandonato.com)

## Trials

Case Caption	Court	Client
Bodum U.S.A., Inc. v. A Top New Casting, Inc.	U.S. District Court, Northern District of Illinois, Eastern Division	Defendant
Coty Inc., et al. v. Excell Brands, LLC	U.S. District Court, Southern District of New York	Defendant
Christopher Lewert, et al., v. Boiron, Inc., et al.	U.S. District Court, Central District of California	Plaintiffs
BuzzBallz, LLC v. BuzzBox Beverages, Inc., et al.	U.S. District Court, Central District of California	Plaintiff



## KEEGAN & DONATO CONSULTING, LLC

31 Purchase Street, Ste. 3-4  
Rye, New York 10580  
914.967.9421  
[www.keegandonato.com](http://www.keegandonato.com)

### About Us



Mark Keegan brings a wide breadth of experience to Keegan & Donato Consulting, having spent over a decade formulating case strategies in complex litigation. As a founding partner of Keegan & Donato Consulting, Mr. Keegan has actively consulted on a variety of litigation issues ranging from marketing and international business to consumer research for Lanham Act claims.

Prior to his work with Keegan & Donato Consulting, Mr. Keegan assisted a diverse range of companies as a marketing strategist and operations manager. From working with top brands to create innovative online advertising solutions to positioning and communicating a company's competitive advantage, Mr. Keegan's practical execution of successful marketing strategies has benefited several organizations.

Mr. Keegan received his law degree from Brooklyn Law School (1995) and is licensed to practice in New York and Connecticut. His undergraduate work was completed at Pace University where he received a Bachelor of Arts in history.



Tony Donato has served as a consultant in complex litigation matters since 2004. He has a broad range of experience in research, strategy, survey design & execution, data analysis and case management. Mr. Donato has consulted on a wide variety of marketing, intellectual property, and consumer behavior cases covering trademark, copyright, patent, best efforts, advertising, business damages, consumer surveys, business ethics, and other issues.

Mr. Donato has a strong analytical background which he developed in his prior employment as a member of the research team at Harvard Medical School's Division on Addictions. He is the co-author of several peer-reviewed journal articles.

Mr. Donato received a Master of Public Policy from Georgetown University (2002) and a Bachelor of Arts in politics from Ursinus College (2000).

## **Exhibit 2—Documents Considered**



**KEEGAN & DONATO**  
CONSULTING, LLC

Documents Considered - Chasom Brown, et al. v. Google LLC
Third Amended Complaint
Expert Report of Professor On Amir with Appendices and Production Materials
Access granted to all ILS "expert level" documents
All documents cited in Keegan Report footnotes
All documents cited in Keegan Report Exhibit 8
Brown v. Google - Schneier Expert Report.pdf
Calhoun 340 Mtn to Certify Class.pdf
Calhoun 429 Cert Opp.pdf
Calhoun 484 Reply re Motion to Certify Class.pdf
Chrome Privacy Policy (May 20, 2020) (GOOG-BRWN-00000930).pdf
DE 113 Mar 2021 Order by Judge Lucy H. Koh denying [82] Motion to Dismiss and denying [112].pdf
DE 113 Order by Judge Lucy H. Koh denying [82] Motion to Dismiss and denying [112].pdf
DE 136-1 Second Amended Complaint.pdf
DE 363 Dec 2021 Order by Judge Lucy H. Koh Denying [164] Motion to Dismiss.pdf
DE 363 Order by Judge Lucy H. Koh Denying [164] Motion to Dismiss.pdf
DE 427 Administrative Motion to File Under Seal Opposition to Motion for Leave to Amend Complaint.pdf
DE 427-1 Declaration of Jonathan Tse.pdf
DE 427-2 Proposed Order.pdf
DE 427-4 Exhibit 4 - redacted.pdf
DE 427-6 Exhibit 5 - redacted.pdf
DE 427-8 Exhibit 9 - redacted.pdf
DE 428 RESPONSE (re [395] MOTION for Leave to File to Amend Complaint.pdf
DE 428-1 Proposed Order.pdf
DE 428-10 Exhibit 8.pdf
DE 428-11 Exhibit 9.pdf
DE 428-12 Exhibit 10.pdf
DE 428-13 Exhibit 11.pdf
DE 428-14 Exhibit 12.pdf
DE 428-15 Exhibit 13.pdf
DE 428-16 Exhibit 14.pdf
DE 428-2 Declaration of Stephen Broome.pdf
DE 428-3 Exhibit 1.pdf
DE 428-4 Exhibit 2.pdf
DE 428-5 Exhibit 3.pdf
DE 428-6 Exhibit 4.pdf
DE 428-7 Exhibit 5.pdf
DE 428-8 Exhibit 6.pdf
DE 428-9 Exhibit 7.pdf
DE 460 Administrative Motion to File Under Seal Reply in Support of Plaintiffs' Motion for Leave to Amend Complaint.pdf
DE 460-1 Redacted Version of Reply in Support of Plaintiffs' Motion for Leave to Am.pdf
DE 460-3 Redacted Version of Exhibit 2.pdf
DE 461 REPLY (re [395] MOTION for Leave to File to Amend Complaint (R. CIV. P. 15(a)) ).pdf
Erdem report - Calhoun 427-6 - Exh. 4 to Trebicka Decl.pdf
Erdem Report (Calhoun).pdf
Ex. A 2021-04-09 Brown v. Google SAC-.pdf
GOOG-BRWN-00028191.pdf
GOOG-BRWN-00042388.pdf





**KEEGAN & DONATO**  
CONSULTING, LLC

Documents Considered - Chasom Brown, et al. v. Google LLC
GOOG-BRWN-00042388.pdf
GOOG-BRWN-00406065.pdf
GOOG-BRWN-00441285.pdf
GOOG-BRWN-00475063.pdf
GOOG-BRWN-00477510.pdf
GOOG-BRWN-00555223.pdf
GOOG-BRWN-00806426.pdf
GOOG-CABR-00084985 - Native.pdf
GOOG-CABR-04400001.pdf
GOOG-CABR-04400002.pdf
GOOG-CABR-04400004.pdf
GOOG-CABR-04400005.pdf
GOOG-CABR-04400006.pdf
GOOG-CABR-04400021.pdf
GOOG-CABR-04400027.pdf
GOOG-CABR-04400029.pdf
GOOG-CABR-04400030.pdf
GOOG-CABR-04400032.pdf
GOOG-CABR-04400033.pdf
GOOG-CABR-04400034.pdf
GOOG-CABR-04665130.pdf
GOOG-CABR-04665136.pdf
GOOG-CABR-04665141.pdf
GOOG-CABR-04665148.pdf
GOOG-CABR-04665156.pdf
GOOG-CABR-04665164.pdf
GOOG-CABR-04665171.pdf
GOOG-CABR-04665175.pdf
GOOG-CABR-04665178.pdf
GOOG-CABR-04665183.pdf
GOOG-CABR-04738550.pdf
GOOG-CABR-04971904.pdf
GOOG-CABR-05477364.pdf
GOOG-CABR-05836882_CONFIDENTIAL.xlsx
GOOG-CABR-05876970.pdf
GOOG-CABR-05876977.pdf
GOOG-CABR-05876987.pdf
GOOG-CABR-05877005.pdf
GOOG-CABR-05877011.pdf
GOOG-CABR-05877015.pdf
GOOG-CABR-05877023.pdf
GOOG-CABR-05877032.pdf
GOOG-CABR-05877040.pdf
GOOG-CABR-05877049.pdf
GOOG-CABR-05877056.pdf
GOOG-CABR-05877221.pdf
GOOG-CABR-05877233.pdf



**KEEGAN & DONATO**  
CONSULTING, LLC

Documents Considered - Chasom Brown, et al. v. Google LLC
GOOG-CABR-05877325.pdf
GOOG-CABR-05877511.pdf
GOOG-CABR-05877813.pdf
Google internal survey 2018-08-022_Incognito Metaphors_GOOG-BRWN-00042339.pdf
Google Privacy Policy (July 1, 2020) (GOOG-BRWN-00000239).pdf
Google Privacy Policy (March 31, 2020) (GOOG-BRWN-00000209).pdf
Google Privacy Policy (May 25, 2018) (GOOG-BRWN-00000096).pdf
Google Privacy Policy (Pre-to-Post Litigation Redline) (GOOG-BRWN-00000589).pdf
Google Supplemental R&Os to Pltfs ROGs Set 9 [No. 40] (2).pdf
Google Terms of Service (March 31, 2020) (GOOG-BRWN-00023941).pdf
Google Terms of Service (October 25, 2017 to March 31, 2020 redline) (GOOG-BRWN-00023967).pdf
In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020).pdf
Incognito NTP Message since 2016.pdf
Reply ISO Mot. for Leave to Amend_ Without Highlights _Filed Under Seal.pdf
Search and Browse Privately (GOOG-BRWN-00024215).pdf

### **Exhibit 3—Amir Studies—Open-Ended Coding**

record	uuid	QF3r1	Code
1594	g2q51937duq5690h	A claim that personal information had been leaked without our consent.	2
126	ufa9kuz1duzpxxjs	A litigation or action brought in a court.	
945	64znjswx6cetwyg2	all times good	1
1620	9wpguy78djwbj1ux	Brown vs. Google LLC	2
2384	6c5qyq9mp8n0b7xf	Claims against Google using information obtained in private browsing	2
2409	vkd2ensx9cbda5s8	Companies using data when they're not supposed to	2
1289	dm2r2ckst28q12qw	Copyright infringement,	
782	kxdrm40p9nerpzuf	dfddfgdgdgddfg	1
548	amw5jsc0r7qwythv	Dog Bite Lawsuits	
1256	h7236pdk9190us2b	Don't know	
1281	w4fxv8uv2xg9afjv	Everything very good and very nice 😊	1
1373	xwzam4dscsf5ab1x	excelent	1
1408	wqa0jdu2qjr4j98e	firefox	
1359	wjb0dsryc6zq51bp	Firefox all of it great	1
1423	eq862mezzu19aa2b	Fraud should be restricted	
911	256jam4aep5ccgpa	Good	1
1454	emcr18hnrtx6tc0p	GOOD	1
719	mwjkkvvry6x9t3vz	good mode	1
1421	5an1aemb8u0yn0sx	good, nice, cool, better, fun, easy	1
1617	w4bvbb67s9fa76e6	Google chrome	
2428	kgefj5zbh314pbmc	Google selling private information	2
1632	p5ku4bq6pezhx0em	Google spying through google analytics	2
124	r8es6z2w1py819dk	Google tracks users even when they are not browsing	2
271	f2uaztxfebhnrdn	Great	1
1508	q25wft1nyrkdmgt	great	1
45	vyd9b77sn3sbzzja	Great	1
272	cuwg5zjwg1srbrt0	I am aware of the brand.	
1120	qxmvc2qq8wxvhffg	I am aware, I know there is one right now and then more to follow.	
1449	eawrmp89e71t58aw	I am suing the entire reptillian race.	1
88	5hj6s4xva12y2ytu	I don't know	
1730	9aa7w9h815mz325z	I don't know much about it but it was a lawsuit that revealed that Google collects data from incognito and ever since I dint trust them as much.	2
1322	5uazdt873nsfpczh	I feel like one would be that the things you searched up, since it was done in private browsing mode, can not be used against you in court since it wasn't supposed to be seen by others in the first place.	2
1395	na5x4w9thgjfbjxs	I know there are some but not specifics of one case	
1249	8zn52x6wxm9phnrn	I like	1
1664	e7tjmvh1k01mfqc	I remember hearing someone sued Google over thinking incognito mode was 100% private or something like that.	2
1644	t8cndyw6ptvztnbv	i think good	1
1582	kbmtvj7wehvc3t4	i think it is a good thing	1

record	uuid	QF3r1	Code
756	0je0dd0k5ds3q87x	I was always take care about this details It is so important for me	1
1413	9um6tz1kboxatfpsb	I was aware of the google chrome private browser mode lawsuit. Supposedly that google chrome's private browsing mode wasn't so private.	2
311	b6bfb0am1r5r4z1u	I WAS VISITING A PORN SITE	1
865	wth2s2pkd5qbktwr	I watched a documentary about Google being a risky platform for private use. I'm not informed enough about the details of the case.	
28	fee36efwxy88sn99	Idek tbh man	1
853	20wbm2eyn977mgaq	if they share other peoples information	2
807	hf049hc3pux7vn0k	In 2020 google was sued for a 5 billion dolar lawsuit on the matter in question	2
183	b1pttxk9kh1p8cv	inappropriate websites visited by minors	
725	ma1d8rvgy73vcjz2	INGONTIC	
884	kw9x1m5bq39eftxu	Is very good	1
1703	m63uhyesrcxmg21	Issues with the seller	1
1438	wjpx8hwu3pzzg3c6	IT IS GOOD	1
304	1hkpbjnnsujvm78x	It is good and u are you doing today now he did not have data and on the bed and I will be	1
1583	9s68nndyhj13a18v	it is very good and funny for my familya and my sister	1
875	nxfcfqvxjkyhybnb	it is very good i like it a lot	1
988	kqme1qr4tqqr3w97	IT IS VERY LOVELY	1
1568	hsg0532etsntj755	IT SEEM DIFFERENT	1
864	2e66btd2tars4jdp	It was a lawsuit against Google for tracking you through private browsing	2
83	82q72tsjn1mtawm7	It was not well attended to for it was lacking enough evidence	
1638	zr368jwf66jwd341	It was very favorable	
536	ubxfz4600veewa1s	It's safe	
1000	1ghk7a5rndnzz24z	Its much more good way to this so I like it much more.	1
1771	xfp3t2tz1db016gw	It's not just the first	
990	v4q1jkpnx4pxferj	It's very good	1
1575	1903f4fgxpdhcgjg	LAWSUIT REGARDING TO PRIVATE BROWSING	2
732	dgsbrt0yjxb8nm24	lawsuitprovide is very good and easy to work	1
752	bbzhzjeq7q9v8d64	many kind of	
1642	3vbywcue15qdgegp	mt internet service provider does not receive my data while i am using from private mode.	2
136	xy351ak03myuzrnm	My lawsuit regarging is the best idea in this option	1
957	b68y4zbs2t0zftxq	none	
740	6nyjamnmcy9kw1qj	not sure	
430	nh49cwzkja16um81	Not to disclose or share any content	2
1736	cx167ncwdbzgu91	Nothing	
2227	75synv5kj5w2g17q	Opera	
237	jf6enycp89wupkw9	OVERALL ITS A VERY HELPFULL	1
805	6a6byhcyq25qbg85	People filed a lawsuit because people said that google was still keeping data on private browsing.	2

record	uuid	QF3r1	Code
319	6utqmyq43ggjzmmq	People V Microsoft	
67	bx4rfmwj0pwerers	Privacy infringement	2
1888	spd530xheuej8sn5	privacy terms have been secured	
963	0339m2uz22ebm7m8	Robins	
879	pw54r38mn670cjrj	safari	
129	vggbsbw1ygc8xvbu	Security	
983	2eps3twgb6bfu0tq	Selling our data	2
156	y66btaw7a7qndh31	someone i knew was getting sued and didnt know how to go on about certain business when someone was ordering with that	
1429	d2vmuw2c5zp1uew7	Someone sued Apple because the website came up	
1415	rm4eq0ze9hxxf768	SOMETIMES IT DOES NOT LOAD THE IP THAT IS	
844	k89pgaxfamf88udu	Still, in 2020, Mozilla Corporation's revenue was \$466 million from its search partnerships (largely driven by its search deal with Google), subscriptions and advertising revenue	1
1049	xfuat8z106ezd92y	The internet was still able to see what i was browsing	2
539	99cwbfc8ma4bpnu	The law suit make everything more private and easy to use in order to keep private and all needed information being placed in needed places	
1253	f5fqg6g2utnqpnsb	The lawsuit that says things that are copy righted and other things such as privacy acts	
1052	hyut095q0wk419ax	The people who owns the internet will know the private browse history	2
778	ynpzuc5efv9u96p7	They do not collect any data while i am in private browsing mode.	2
974	mtnv4g0bjv5vymgg	They re dealing with my private data like when I am in private mood any company will not be get my data as like I was anonymous to them.	2
1589	7s2886afbba1jxvy	to give privacy	2
1805	fwchfrwbf0bw99ts	Unsure	
2466	whtyc6rt3spr9bg0	Unsure of details	
928	190hnhvf4m9betdm	UTE law	
1392	vf1k8fev60jsw74m	very good	1
600	4qx785tyx1drqv5b	very good	1
1015	rr4aejjq68q0fzyg	VERY GOOD	1
1555	h3mghcp7s62wsn54	very good value	1
434	ct4y5qekhq8rev4c	Very unique and innovative products	1
1621	7r661c781jwj0m4m	VERY USEFULL EVERY TIME	1
1643	5jy9ut5d6dt3n3d8	Visit adult site	1
1814	r8v9tfefnbwsg4vk	We have to be careful against hackers	
1503	qbk92qzu7x8fvrkv	Yes I'm going to get my hair done today and I just got home from work and I just got home from work and I just got home from work and I	1
1034	jpkf8rdy3vaskzy7	you can't use it with government's sites	

record	uuid	QF3r1	Code
639	2ce91bzgm2ww18ne	2020 google faced a demand of 5m \$ for information tracked in incognito mode	2
4555	tu87cvkz47qpmzt7	A lawsuit was filed against Google claiming they can still monitor locations even if you're using incognito mode.	2
4377	y4k3y64c1p9fm6vz	A lawsuit where all of this info was false and Google can see everything.	2
4064	8316y92sewfn8yw	afsdafsfdsf.dasf ads gfdsf sagdfgwdsaf ew.df af to long.	1
599	y9xs861jzd1b6dq4	ALL IS AMAZING	1
1533	ty5tjebv6qx1xyt2	Amazing	1
4478	74fgkzhu526ub2kx	Any lawsuits	
17	mu9va875hqm0fste	Arrested	
1348	5k3rqgdnkbf0fb40	Best concept and very interested	1
907	7dgwy6v30et4ek0s	Better	1
34	7jhpc5akr98azqj0	Better understanding	1
4563	uc8vsj95tm91h6q9	Chrome	
4752	3th2696c39cqznut	Chrome	
3123	t7g7zmf7hkhhd8v5	Chrome will not store the browsing history, Cookies and sites data	2
2532	rqd6hj68q5ya03at	confidentiality and privacy of browsing	2
1129	ee0427yt5xgpy6f7	Copyright	
1768	e7fzc7vqmpc1j7gx	Copyright us a non no	
1496	0bv1gbvy5efy42kw	Crimes can be tracked	
3981	d0ys8m6jbn3yr5am	dfsdfsdfsdf sdfsd fsdfsdf sdfsd sdfsd	1
2860	wm6xuawvgvjb93b	Don't know right know	
4599	shpm1p3j0gare6z8	DON'T KNOW	
5145	64aatbkh1vr0s2t2	Don't know	
1803	rrspen7uqzux5qhw	don't now	
1798	552zp5mbmqsd8c14	Everything	
3918	bf1x84qqn19ss0fh	excelent	1
5574	xjrp8fgav859ybnu	EXCELENT	1
1495	hg8wwbb2z5nuaq6x	excellent	1
2370	k1tarm4gswzfrg5g	excellent	1
3563	mfa12z62yyu2ewdh	EXCELLENT	1
3336	z6s4yg8m0qnmr98u	Excellent and very good this browser.	1
913	vtcbm89wzsq7g7av	Excellent and wonderful great unique different from other products very reliable and trustworthy	1
3153	ef60amndkk7a5w0n	excellent mode, I like very much	1
3192	3bfrtjc2qbcakef5	F GD FGDFGDF GDFGDFD	1
1759	4h40wdf77v94m87m	Fake Ip address must not be in use	
4445	bjebqd00pg7wvmrk	fdfsdfsdf sdfsd fsdfsdf sdfsd sdfsd	1
3991	d8dq3yfq49g43pj0	fine very good	1
5293	avuuq2e5e42e7cs92	Fraud	
2397	erjevs20p8mr9nqj	GOOD	1
2530	0snppnzeef7422xg	good	1
3086	6ff8znqcmw5fcdq	Good	1
4771	rqtbkxdqjum7b1j1	good	1

1 = Low quality response

2 = Knowledge of current lawsuit

record	uuid	QF3r1	Code
192	7znv8fujc1gfucwj	GOOD EXPERIENCE	1
3191	xh65n5w4mu5ajky4	good lawsuit	1
1352	vshnj44jh0cx29v8	GOOD VERY GOOD	1
3089	w2rymn5s3hy5c9yy	GOOGLE	
4270	m5w3mc2gym8bxgrh	Google	
4336	q1mg2y4kf8akpwhh	Google	
4370	z466a93859gms3s5	Google	
4523	8zus9zukf5dzc4kc	Google	
4074	uvzb08syppad8bry	Google being face with lawsuit over tracking their users in private mode	2
3654	nc96f0f4vm8agy3f	google chrome is very unsafe on the info	2
2694	8t1295k3ra90nq4q	Google does not receive the websites you go to on private mode.	2
5618	12mbemw8sx1unnrb	Google had a lawsuit against them for tracking in incognito mode	2
3661	feb0gck1nr9au938	Google has Many lawsuits	
1333	g367m8ckkh3uxtr	Google is a great provider	
3482	7xxh3rts044bg8ja	GOOGLE LAWSUIT	2
1005	fc7kbz1zwyqur4n1	Google security is most secured.	
4060	49ghc7w1jjwd6a8k	Google still gathering information from incognito	2
4564	wpjzpe0uhxj30fdv	Google still might see what you're doing even if you using private wen	2
1212	nt99xmf9pjs6pqbh	google truck user	2
3116	5krzdqubhtjb091t	Green	
1559	wbpd0z78zxcdtwx5	Guest mode	
4319	pkkeh6n15975n5dy	Heard it wasnt that private	2
1827	xh3asbjd3c2hez50	Hedjk and night in the next day and ktexjk in the world at all of the index finger and I think I can get the first place	1
308	bjputkttrsvbr08g	Hey buddy I just got home from raider I love love you mama bye mama mama mama	1
2769	mh9ws2bjdgyr5srx	hmm isnt the lawsuit like the policy of the each site	
1347	56tfmf3cd9a3z4de	i already know about the private mode	
1463	47y8frjbxh1hn105	I browsing a address for shopping	
1044	u8x21jmcdm6eqp3v	I can get you anywhere lol lol	1
553	rxxxk72kxwtt60db	I definitely for sure have no idea right now.	
4613	k5bs43s9fb0fdu5k	i do not know	
4486	8a0zqst8secu63ae	I do not know any specifics but I have heard about data breaches and potential lawsuits	2
5656	b1940vr04p1xpr67	I don't remember specifics but peoples browsing history was being saved and info was being used	2
1927	mj5427vrr6hbhrdk	I heard about one stating that incognito mode was not entirely private, and Google still got the information of the user browsing in incognito mode.	2

1 = Low quality response

2 = Knowledge of current lawsuit



record	uuid	QF3r1	Code
1506	24nxzz8hbs18653u	I heard an individual was trying to sue because he was watching lorn in incognito mode thinking it was secure not knowing his wife was able to pull up the site and this led to a divorce	2
1218	e2n4h30z7eg4y86j	I heard or read about people suing sue to incognito mode not truly privatizing searches from ISP.	2
687	apy6zkk2d2abnchn	I HIT THE WRONG ONE I MEANT TO CHECK NO	
1206	wf8xuuvxbd2qgbma	I just remember seeing some thing on the Internet I didn't pay attention to much of it at the privacy laws are being questioned on Google	2
68	1s8nyrq43zub9tx5	I know that Google can see what you search up and that you should be careful and stay safe on the internet	2
5153	t4r77k180hrymg8a	I know there was a case they can look up by your IP adress	2
1800	vzxhhtctvqtxs6gt	i LIKE all mode	
3566	37b4ggve2w6uwfrs	I like chrome	
325	719we3nkwg3xevd3	I like so much, I love it	1
429	je1vgd8hg5ktg06	I like so much, I love it	1
3621	p4kznqdajqev1v6k	I like to browse privately	
1114	u0knf6v4ratetwfk	I like very much this service	1
946	uc87scw8wsaxu9yt	I liked this browser mode, I think it helps to avoid saving temporary files that harm operating systems over time.	
4253	7aqt6rk3g6mtwtty	I LOVE USE THIS WHEN I USE SITE	1
1378	h8fjdvyubscgtvxe	I MY PRIVACITY DOES NOT PRIVATY-	
1529	arpemew3tzbgbn2	I prefer to keep this to myself	
4698	azr9azzsedv7gss1	I SKY	
1507	9wtb43jvwmmchpvc3	I think its a great idea i like it alot	1
1257	dkusuxxpm5vrvfd0	I THINK ITS A VERY help full every time when i use a private mode	
2821	9p4kn0kqkja1apz	I think there's a lot of things to do	
372	1duty2z3zk3hfc5n	I use this chrome in very moment for the privacy	
227	7kfnp26ndvzbv64b	I VERY INTERESTING	1
1377	zg8mbw0pdm2k8cyw	I was are about lawsuit	
4160	7sge00n647gv8m5u	I was aware but now I am not anymore too sad pepaga	1
1267	63sc3wcwj07bp79j	I was aware of a user sewing Google because Google chrome missed up there phone	
2799	j11r5u9y7edjwgr0	I was aware that it does collect some information.	2
4235	3hpteuepb1a9pwaf	I was aware that recently Google was accused of still allowing advertisers to collect data even if users made actions to prevent them from collecting.	2
1091	vxcxjaetfuy42axu	I was getting sued for rear ending a car	
4259	bbdcuqp9dk84v989	I watch it on TV	
1330	6dn3r89k022ywww0	I'm just leaving my moms now to go home so I'll see what wtime ryeoryeie El'm is not mad at me either but	1
3545	k2uzmd9wga3hfrcj	Identity theft	
2449	9gm7ay7kp35psfkd	If there's any copywriter	
1595	6pjtrgudjuwf5z64	I'm concern about it.	

1 = Low quality response

2 = Knowledge of current lawsuit

record	uuid	QF3r1	Code
4433	5y2st6t0fcx1rez1	I'm not sure of the specifics, but I remember Google got sued for using people private browsing data for ads.	2
4440	j445tgnt34v54na5	I'm probably aware of this service.	
2006	fr9u9zuvbtb1wspm	Innovate plus	
3851	ctzey3p3dcn4q06y	interesting and very good	1
4075	vkfx629qsxk8320z	is good	1
3924	yrp0vc1dn4gvqw1x	Is very good	1
294	bnnz29q85y4bu33f	IS VERY GOOD AND FINE	1
3131	wqucdjvrq5w2du0f	is very good google	1
1789	4uuhb2ca09t7xzmw	is very important the information website	1
3618	djc66q9p3xt0g4w9	is very nice	1
4032	k2gtbbvsjbf6z54b	Is worrying, the privacy and use of the data collected	2
4702	6vg88jd37gbsrsbz	ISKY	
2551	y8chkfkswz852yw3	Issues back in 2019 with security issues	
2348	g3tv88b4vqcgtyet	it had lawsuits over google stuff and legality stuff	
1477	q2yse4zj152jf18m	It is a very good company	
998	cjhsg6ztxnferb0s	IT IS GOOD	1
4519	q1y808fke0sx9nms	It is part of my digital awareness to properly use legalities associated with the account.	
1259	v3j4rhb76k5dvwc4	it is very good	1
2618	49xj591vusfprpz5	It not actually being private	2
2440	s5xu182y7ezxz23m	it seems that it was not incognito	2
686	xb5cvyjsr03wugk	It was dealing with third parties which was basically written there and they were one more thing they are making our browsing more sure and easy.	
1821	pmz3sautk9fehpx3	It was good	1
4124	1uu5q44n55sb1zem	It was pretty obvious	
1429	bKz8zrx9d8aanjq9	It was very clear	
514	eb3xw8a2q739jap0	It's a thing in the browser not sure what to say	
1004	a62uea79j74y97qa	Its a gogle layout and which is good	
578	feyacrup42qf4kur	Its better for cyber security.	
49	3deu4qqzdsyf40cs	its good	1
1227	724zh19k0kqgcpcp	It's good for all	1
1028	wjvjp0t65hjux5xy	It's very dangerous	
185	a548bea03u0u8n82	like it and good it	1
1396	7pygz6nh58mb9pwu	like to agree magnific	1
4658	pmxedgpbzrmwn6j	likely	1
1203	a3kr06cbhpgnm4he	mention ed something about ip something tat i was clearly aware of	
3468	pg4zqjjwz44umjzn	Mode incognite in google chrome	
4667	yj3ca7xnuszs006j	nice	1
4736	w9dqrkw9hyek4v36	nice	1
4755	pu5j9ychgpwa1rvn	nice	1
4773	rsw8zxv9sz2smkep	nice	1
1815	drnjrk9z6spzq82	No browsing history	
4244	5dzpqsp2hm0qj1c9	No crime against humanity type searches	

1 = Low quality response

2 = Knowledge of current lawsuit

record	uuid	QF3r1	Code
4383	wunr46x0kapw6wse	No hAcking Privacy rights Underwriting	
2592	ugw215t2gnt78w0q	No history in the pravate browsing mode	2
1536	senp07q8csb4zksw	none	
1766	e802e63xk1dfbmy4	None	
1853	4h0e7k9apudxq04w	NONE	
554	vx5x1gdac64gc58k	not sure	
58	u47qkkn07yb8y2vk	Nothing really much the law suit was thrown out	
4163	z0vs7pb6sdhm55x4	People complaining google was tracking people policality what they were doing	2
3379	kqtn0y75hqct4na	People fighting against reading of personal information that was not provided by person	
1083	ghgqz1s0u7fv7dpf	Personal information	2
1046	ywz0rxjqx8ejpue	Privacy concerns over browsing	2
3181	qzss2hhu31hr2dxx	privacy terms	2
4531	afet035tgffpeyh1	Privacy thift lawsuit	2
628	6tht4m2bhq260x3x	private browsing isn't actually private	2
5527	jksy7xbua807r4x	Private mode is to be unseen. That's interfering in someone's privacy.	2
1790	7td5jfbqrp5g9y94	Probably google does receive this info	2
1497	x2qj10mfgfuf0dhf	Probably like Youtube ads on Google	
296	5gfrwbnrbejf6dgr	respect for privacy	2
3669	ycf2x7rfew9uknnk	SDA DHT CIUYIUY IU Y IU U YLI YL	1
3495	m9arue981s6b67tp	security breach	
4789	swees3mzfga81bhk	So good	1
1123	4w7qg9ffy587u09w	SO SPECIFIC ABOUT IT	
1843	2sw0y3442v1x96ac	succi Les aig guy	1
1785	hmt56wjscz390qf0	THAT IS VERY AQMAZING AND REALLY LIKE TAHT. THAT IS VERY USEFUL AND HELPFUL FOR ME	1
1293	hmdapxkhezt7xx79	That is very secure and innovative	
508	u231b5fss5q25kfy	That you can still trace the IP address when you browse in Google chrome	2
1153	x46dk4y22gy8sdfg	The Google lawsuit	2
1854	m9yt3cm1qtzec32q	The I have to get my stimulus it works for me	1
1394	qpme pb5qzubaz8zv	The internet is slowly	
22	u0uhgrd019k7ufc0	The lawsiuts are so ffod and very protective in cookies information and giving good experiencs	
355	1bfijk2b9xxpfaep	The lawsuit contends that chrome's private browsing Incognito mode should also stop Google's server side tracking and that Google's failure to cease such tracking	2
993	bucrctuz8g61duhd	The lawsuit of being spotted even through private	2
1010	tr59pqyc1h3qhhd4	The lawsuit, filed in June 2020, alleges that Google tracks users even when they're browsing in incognito mode	2
1403	ff71f6g6avecnauk	The lawsuit, filed in June 2020, alleges that Google tracks users even when they're browsing in incognito mode.	2
4351	v0x6cf0r83avtmap	They have good options for the people and need a best page for the college	

1 = Low quality response

2 = Knowledge of current lawsuit

record	uuid	QF3r1	Code
4510	gcrtn2hahpgt3ay3	This is a unique browser	
3156	8s9bhppgejwbxyq2	This is so good and very likeable	1
1455	8rhftfjmxz4ayud	to give and be given in return.	
4577	up81ur92u95jcz0w	Trust him	1
3990	gqq5v9k0qyc76tuu	ugjbjhbhjbjbbbbb	1
1814	g2y5sene1vb1w563	Um. I totally thought that question asked lawsuits agaisnt copying this information ... I read that all wrong	
2683	gh1c10fvh67yjk5	un legal browsing	
1388	uz4gvna46setnu77	Understood - a lot of people may have used the incognito mode in the Google Chrome browser, but did the browser actually hide user data? A lawsuit was filed by lawyers against Alpha Bit, the owner of the Google Chrome browser, because of the Incognito Mode, which allows the user to browse in secret, in order to preserve the confidentiality of users, which the lawsuit says is incorrect. The lawsuit accuses Google of breaching people's privacy, tracking internet usage even when browsers are set to incognito mode.	2
3098	c40kf974vmw95f7h	Unsure	
4624	s9h2n09ntppbxjd2	unsure	
4669	36auvnaec0kkupx7	unsure	
487	0z905p9xt4h3a2jr	Unsure of details	
3919	e9v8xntej5qreyk	Unsure of specific details other than some information supposedly not collect or available actually is to Google.	2
3811	f53us0vk1nc14t98	very fantastic excellent	1
450	csmkt3x0p0dqvbni	Very good	1
989	edahwtg7aw98d5xm	very good	1
1213	3j65n6vz55jc8ka8	very good	1
1914	ctd7a4m3fvhc11m9	very good	1
3931	vfauneq1dqpk8utg	very good	1
3977	d7qd1tqmn1ubvc40	very good	1
4000	9cku0za8xnc69egn	very good	1
4223	z1za7u1hs5j79ea1	very good	1
4690	mw9jtt57tc5gn3zw	very good	1
512	cyf4z003zawdxztr	Very good is google	1
2471	wemtc45usmetaev2	Very good is the private google	1
384	vp3dm82fxwhpjbsk	Very good like more	1
559	y1dd4fej3gg1cw9s	Very good like tree days	1
1309	dqy2erbdzn71qadq	very good, i like	1
1424	xd07h6a198bq56pr	very interesting	1
2407	z6xn4vrfsdn1c98	very positive	1
1112	zn6gjsfh0sxt1uyk	Welcome to Gboard clipboard, any text you copy will be saved here.	1
3561	r388g7x3mwca03vn	YES best	1
4344	8f5q3nrnsnrwsgd7	yes very good	1
208	68zjuspvtg8w53j	You share info your done	
2921	ymeddj7ducv5uepe	Your cookies and history isn't recorded	2

1 = Low quality response

2 = Knowledge of current lawsuit

record	uuid		Code
4573	5mr9w0fsw8cqd8v4	Your internet provider may still see your content	2
3129	p2acuxjtarxmzy98	YRD BEST	1

record	uuid	QF3r1	Code
2657	a77rheuz6d0w2zwa	A California judge has filed a lawsuit against Google, alleging that the search giant secretly collects data from users even in Incognito mode. Three users filed a complaint last June claiming that Google has a widespread data tracking system and continues to track even if users take steps to protect their private information, such as using Incognito mode in Chrome or Safari and other browsers. According to the technical website The Verge, the lawsuit seeks to impose at least \$ 5 billion on the company.	2
3210	27wnu1532135hy0b	A LITTLE SLOW	
2375	82puww8mzchk9qjd	About high quality of the chrome	
3622	9sxbxadzvtp7tfm	ABOUT THE CHROME	
3478	53eavqse4mjtgnsp	all is very perfect and very nice	1
2019	jvw1tyw72k492682	all of it good	1
4092	rmwyu9c5b51e6f28	Apple vs bannana	1
2024	nqsg6h57ypj222	Back page.com vs Washington State	
3270	hg6rjdjnqdg4cafb	Be able to broser the net privet	2
2083	r161ywhzb9mjh3z	Because they are very innovative and trust that they provide us good services all the time very much Highly.	1
3233	ktpg22stqbbpbdn9	Best	1
4101	0ne1bpge6jgghnfn	Best browsing and very interested	1
1899	337s4cyq4nqgcmar	Best of the best with zero issues	
3996	0pabrwyqrru8xkpd	Better understanding	
298	m2nmsfjtk5745xqt	BROSWE A LITTLE MORE PRIVATELY	
442	4cnng09h27ac7dha	By facebook	
3610	yb31v33qbd4u2ckb	Can't remember	
818	xnep6ws5bsfsrd4y	Chrome	
4140	u4vmkta6pzt9wtxe	CHROME	
466	4x3t9wwwbjejn57d	Chrome launce a private mood	
699	fp17kgq90mf6yqa1	Consumers filed a class-action lawsuit against Google for collecting data while using Incognito mode in the Chrome browser	2
2374	dtdqx09kx2dz3ne0	Cool	1
1893	6y5wvvv60wtz90k5	Crime law	
1898	tvfzjma1yguhtqr	darj mode	
4246	hsa7xuvkkvmffg3h	Data filtering.	
153	tw65ufmsa1ma4y2w	desktop	
758	x1v4xa888r2qb1k6	Dj and get it done before you go home and I will come by tomorrow to get the room and I will come over and see if I can go to knabe nd take care h and get it evening vena I have to go	1
3829	zvpw6stxpdhggbc	Do not steal user information	2
2358	mr91sb9ku4pmpdcc	Don't know	
1046	wr363fqese7c14jm	Don't know	
2869	4bnfbbcc9qxr71vx	Esse aut saepe autem	1
2199	gw45cd2vbx8phzy0	Every thing you browse on google is protected	

1 = Low quality response

2 = Knowledge of current lawsuit

Likelihood of Use Study

KEEGAN\_EXHIBITS\_28

record	uuid	QF3r1	Code
4193	c2fv3anr8n7u49e5	EXCELENT	1
2380	9wt0egm9cqwnrb5w	excellent	1
4294	z68w95afv2kg134t	excellent networks	1
235	g574ejn318qac9va	EXCELLENT THE BEST	1
1463	z3vb7fd9aqacac82	Fggddffcvvxxxxcccccffggggggggggghhhhhhhhhhhh	1
3983	wuwakgax6sjx7ay9	Former employees	
2341	k2bv3ffjx2sa103p	Giving out personal information	2
1233	uwrc40zx5hbetx4f	Good	1
2423	f2xw049x8wy3jf5e	GOOD	1
2909	vdfu8xz18fjbrcfz	good enough	1
2770	5a65mj6t7c0wgr4c	good experience	1
2824	u6f2wb7h46538cjy	Good ideas	1
2276	8jkqy4vpk8dfescq	Good job	1
3393	vyk3enr1u269udsu	Google accidentally giving out info pertaining to it's users of incognito mode	2
4291	ah0nwp98x8q639xg	Google is ordered to face a \$5 billion lawsuit alleging Chrome's Incognito browsing mode collects users' web	2
66	3a7nqcf88ds4byr9	Google still track user's browsing data in private mode.	2
3474	74c9szdc9cqfv5hc	Google supposedly shared private information that it said it would protect.	2
4085	rschg0zh9na90m4k	Heard of Google analytics leaking people's	2
1431	6fmfhaj2bmdt333u	How to get the kids to the kids to the	1
2345	qj9be5cvv1ghkd0p	I already knew something about how incognito mode works	
3367	r24aes5712g1vnn1	I am aware of a lawsuit against google alleging that they still collect user data even in incognito mode	2
802	x3ybjgw51thcj9u8	I am aware the tools from google chrome	
1755	zth9e5u67vsb6760	I am not going for the family time and they have a	1
3615	5y6mqkkz1zd17tgp	i am very aware of lawsuit	
1443	dakjy77gknkumf0h	I can still be view my previous site	
1420	et0xnk215g5pgtp0	I can't go into details at the moment on this situation	
2456	k89018mxwhf6csx7	I don't know the answer to that	
1208	ephcjpeqtbd0tmuu	I heard about it in the news stating that Google might be in trouble	
1855	5e5yuwc8na2q8dft	I hope so fatboy I'm so excited	1
3346	k913079f3w9mwcku	I knew that it was about the private browsing	2
3240	srddquvr98fq1kbc	I like	
3250	cwmrz87ay0zcmrpg	I like it a lot this service	1
3311	6pxqbmnh8hjctru	I LIKE IT BECAUSE IT IS COMMITTED TO SAFETY	
2585	gj43s4kt2gusrtx4	i LIKE IT BECAUSE THIRD PARTIES CANNOT SEE MY INFORMATION	
2089	81fvm2q7dwj0g15w	i like it very much	1
2114	hv0a53jfh4e1az55	I LIKE MORE FOR AND MY DATA PERSONAL	
2805	e4w7daatvjqu0mab	i like that mode.	1
455	m51gfb57beb5vem	i like this	1
2138	cc31fjj7fyk5p4ab	I like to browse in private window	
430	yftp4gwnywdh6dvd	I LOVE THIS	1

1 = Low quality response

2 = Knowledge of current lawsuit

Likelihood of Use Study

KEEGAN\_EXHIBITS\_29



record	uuid	QF3r1	Code
3467	4hh1n9p5smzhgt76	i love this	1
1811	72bdh6jetu6q35wz	I love you too hot to handle Netflix cast and crew of the series	1
2190	85ukh7gmte8mdbxx	I read that there is a lawsuit against Google incognito browsing because some information is still tracked and the statement on Google's incognito page is insufficient	2
1560	jj6sfyvva38wyszp	I really don't know any of the details I'm afraid I just heard it through the grapevine	
4033	k5tnwbxseg1h18by	I remember hearing that so many people have been hacked and needs to have privacy and this what you showed helped	
2454	ze3t5fsqsapzefmq	I SEE THIS BUT I CAN'T EXPLAIN IT	
3312	t6xyp8afqf74e5vu	i think good	1
3370	2p64zwzw2yaxm1m5	I think this is one of best browser currently, I love to use. Incognite mode is a useful tool.	
3918	5fqusqz8p9rww4t1	I used brave browser and it is great	
3204	zjxtx1ycjccxbzqw	I was aware of chrome taking information that they did not tell people they were taking	2
1202	ns3ct2kyqkcr7pun	I'm an unsure	
2280	suj1hj08thb123gu	Idek tbh man	1
3283	qx68pxtt5g0xqjzd	If you go to download certain things your not supposed to you could get a fine	
1637	bgzwpe0ct84mhn8g	If you go to private mode then it delete your search history when your done and it leave no cookies	2
1533	qqk2cseu1jbpg1nn	If you plagerize there info they will sue you	
1240	p22r981u7ebdcrb9	If you sign in to any website in Incognito mode, that site will know that you're the one browsing and can keep track of your activities from that moment on	2
2154	dy86s8w427rcsgc3	I'm aware about at least three lawsuits	
3773	pk82crzc7bahnazy	I'm not sure if the details about who was suing Google, but the lawsuit was about the incognito mode not blocking all of the sensitive data that by design it promises too.	2
3906	g9w598jca5krsy0b	In my experience is very good	1
2832	fge4uxv03fgccv4u	Inappropriate data collection	2
2350	et35jgvaggz9ev35	Incognito	
3556	34svuy7fyvwxffky	Incognito doesn't make you invisible online and websites get to know when you visit them	2
2854	fkk9duejvcytrdrv	Incognito mode protection	
595	e205t2c7vfcs3gcn	information hacked	
2596	pburzg4sk1xvq459	interesting and very good	1
3093	bpe62kt8qebmc0e8	is design and model is excellent for the customer is interesting	1
2135	2j8a1x8cykybac2z	is good because is excellent	1
1190	n1r72xwj656qu2a9	is good becuas is excellent	1
3209	7gu11j6zngvc0xef	is very good google	1
2176	zjykt22kxk91jjeh	is very good to me	1
4180	38utj49vwgpuk2en	is very good to me	1
970	6z0zg0rkxukfwfbg	Is very incredible	1
3921	4m6duumeyvmsvryq	Issues of privacy & security.	

1 = Low quality response

2 = Knowledge of current lawsuit

Likelihood of Use Study

KEEGAN\_EXHIBITS\_30



record	uuid	QF3r1	Code
79	85p7yxffnj2cavmu	issues with security protocols	
3272	cjwsy1e8js6sxsu	it is a great oportunity	1
1822	rck76b12z01matg0	It is a very good	1
2619	byx998jwbr5f3yqz	IT IS VERY GOOD	1
1231	3pvye0kjbv6d99d09	it is very good i like it a lot	1
217	j1bvqryh82ekddcx	it was a very well	1
3483	hmy9ddufn26x8g6	it was amazing	1
1692	bn78xdz8a8g2bhmd	IT WAS GOOD TO ME	1
3890	bpps0930gtesthgb	it was great one for me really i like it so much.	1
1911	jfr6kuq5s8a1e73x	It was on the news one morning	
4132	r4yv36frsmge99yg	it won't save your recent search for the cofedential	
3826	353v09bqqshntzpb	It's great to know more about laws I am aware of it	
2215	04fzsyvmvfjejf8	Its a very good mode for me, I like so much this mode because keep work of better mode possible	1
1842	54mdehxd0hp15xy	ITS A VERY IMPORTING FOR EVEY TIME I LIKE A SO MUCH	1
2610	71ty6acuwg8z9fg7	It's against the law to hide your details it cause jail time	
2095	7ccvb7un9ypy034m	Its good and safe	
1342	eg99kz83rsg9vqdv	It's very good and nice always	1
1628	58m0xcneuaajhbu3	I've been aware of a lawsuit that had to do with private browsing mode with a person that was under the age of 18 years old.	
3850	gqn78tb1yctyw541	I've forgotten how it went down though	
3085	2zqfbmar06360h8r	Judge rules Google has to face lawsuit that claims it tracks users even in Incognito mode	2
4100	ercv5csw7abr9pw	lawsuit can be a up grabber	
2646	kdp0gj1y0hbrjdzd	lawsuit deals with the description of being private verses the saving of some information. claim is the site is mesleading	2
1821	5ydr8tjeh2cbnc2	LAWSUIT PRIVATE BROWSING	2
4201	cq5g73ku402s1ent	Like that very much	1
2371	9z1k9jvdqkvkyw6	Looking up illegal things	
2385	ndrtgv0u61wj6ej0	LOVETHAT VERY TO ME	1
1036	jj32epux0jsanmea	many use it so that they o not discover the things they are looking for on the internet and it can be dangerous	
3164	nzyzz4yxuuh2mpm1	Mecical	
2351	7r6nd3wrw74zt3td	misled	
163	0n64br467p77etwd	much better	1
2289	yjmwbb63akfzatq9	my experience is excellent	1
3964	jsdc6urrgf4af83t	New Orleans	
3181	fx84we37n2nn3z0u	Nice	1
241	6rdb4f7x2ue32jku	nike browsing mode	
2786	evbgm6t5c446awdy	nm u hug sara kmne ki kaj	1
3160	Orzaq2bzhb4mc6ct	Nnnnnnnnn	1
3402	ut4dqbd298mx5rg	No offense	
995	vz4dwej22d2vqs10	NONE	
2822	u0fvftvwxwjwfsf	NONE	
3245	c1gy41vmd54075u0	none	

1 = Low quality response

2 = Knowledge of current lawsuit

record	uuid	QF3r1	Code
4108	0ax0mt4asazmggygh	NONE	
2429	jnms06vmwt6g6yc1	Not sharing	
301	shmagwkgmk75hpc4	Not sure	
4230	vud2rdes4hz1c48m	Not sure really	
3618	utmdq7cr29cq6wj0	nothing any more	
3601	5k9vautaet1dz1vj	Nothing comes to mind	
24	967rj9840yy3b37h	Okay	
2365	9559smrgjtj2pww9	One of the lawsuit that I can't use during private browsing mode is that you are not allowed to do fradualent activites	
3600	rq51pnzzdw2u7fn6	outstanding incognito	
3291	3te9cjgyrrmpsezm	PERFECT	1
1410	nfm5991h8kq5nchs	please I was in my heart is broken heart and soul and friends and family	1
3772	emp899qp4c531jqj	Privacy is our priority	
4093	8pr70u7ubppwaxgx	Privacy lawsuit	2
4197	x0m2u4v784rx9raf	Privacy of browsing	2
3248	vkdpjmrkk61mj69c	privacy protection	2
1738	2s19w3xrbpgfhhe5	Private history	2
2682	jzd7nbfwe5pm1qr1	protect my identyfy	2
2424	yymc7kgepmdupx53	Quality	1
4258	g9c0j074n2vnnw32	Recommended services and quality	1
2417	dcqqrhun77rbtz7p	Revealing of private info	2
991	cxvd6g1uzuv18528	Some information still visible in private mode	2
1757	pv9ch7m3zhvv1rj0	Some of the patent issue	
3015	4zx35sa2nhzmke1h	Someone tried suing google for still tracking them in incognito mode but it saids your information can still be kept as soon as you open incognito mode on Google chrome	2
2687	df8rjpjvddms05c	Sweet	1
1399	p5jkgpgjg8j4rejcc	Thanks for the update and for the update and for	1
2918	5b1mxvkrfwdr2kd0	That google was being sued because they are still collecting information from incognito mode browsers	2
2573	uhce24wzm1te8n3z	That Google was being sued for tracking peoples data while they were supposedly in incognito mode.	2
2845	p4kdhp0j6ykgt19q	That some other sites could still see your information on the dark mode browser	2
3456	dkhfs2y0wew0kn7a	The block and hiding of personal details	2
3802	4kdp4fh7cdxm6fw4	The browser able to track personal info that lead to criminal charges	2
3619	bcjn9md0hu6anj1	The company not allow to use user's cookies as before, if they have our agreement to do so	2
1771	fmwy4969bhjmknz4	The internet deals with alot of people but I think it was between dell.	
3851	k48yc2c5f9wjfwg3	The lawsuit file in June 2020, alleges that google tracks user even when they're browsing in incognito mode.	2
1485	5s78urjeztaaahnf	the lawsuit involving private browsing mode	2

1 = Low quality response

2 = Knowledge of current lawsuit

record	uuid	QF3r1	Code
4019	pbf46ntt1g58vh40	The lawsuit regarding private browsing mode is very relevant for me because I need something different about you is very relevant	2
1916	hq81nk6wyzv2p9p	The lawsuit states that if anyone makes use of private browsing mode you should either be questioned or made to stand before a judge.	
1405	1f9zhug4y6y682rx	The lawsuit was about the Google still saving data that was specific to the user for the purpose of ad sharing and creating algorithms that make the user experience more specific to the user rather than continuing to have unsaved random content appear that's wasn't specific to any users specific likes and dislikes!	2
2653	2g1vv2wzsqkps6rp	The lawsuit which allowed viewers to suspend illegal activity	
2260	xkg0psba0ycq9kvn	The lawsuits I was aware of a civil legal action by one person or entity (the plaintiff ) against another person or entity (the defendant ), to be decided in a court	
1404	gbfvr94pvtrwp1g	The one that is being sued for collecting data	2
2966	gjh0uhgemx0sa25p	There is nothing more or less than I need right now for none of this stuff	1
4128	cd1rxru91w5m4r7u	They can't legally track you.	2
93	khn00vqhrz5qmc4	they is very good amazing perfect	1
4103	b6vc4879zvvp0wkh	This is a good tool to use daily, Chrome incognito help me to browser relax and secure.	
3614	whe5x2094jxvnu4e	this is amazing	1
3064	5cvud9z9rj2zm7y7	tracking and collecting data even when people use the private 'Incognito' mode on its Chrome browser.	2
1412	xd24thagfkupfsxt	Tracking their internet use through browsers set in private mode	2
1415	3v5avwwdbpmeqznzh	Unsure	
1586	77yngyhey9daehjk	Unsure	
2893	hnrj2pjgmyue5r7	UNSURE	
4158	3y0a12v4b6fydxvp	Unsure of specifics. Think it is chrome ingognito	
3230	5tqt6uyc1a752aw1	Using the browser freely and safely	
3024	2ucr5uj2pzvy3u0u	UTE powersuit	
1486	cygv1xc8ymyqvj8u	V. Chug chihuahua. Xryuiin Chuck fgjik chbnkjfc. Stub chuh vhhh. Ddfgbc fun vhhhv. Bhubaneswar. Bj	1
109	w9v310jsatb3wvmq	Very good	1
210	d54824kycjs2452e	VEry good	1
372	vetmb9yj7a7xpr23	Very good	1
1024	twr4espm6tqwdrtdq	very good	1
1197	yx802s8t3rz7vyme	Very good	1
1697	1q3zhe21aj1qbq0m	VERY GOOD	1
2290	xwumequygzcea7z2	very good	1
2382	xdq8rt1eww39k1ub	VERY GOOD	1
4040	3mpwkv64ms2x5d5x	VERY GOOD	1
4186	v07skz565716v4wy	very good	1

1 = Low quality response

2 = Knowledge of current lawsuit

Likelihood of Use Study

KEEGAN\_EXHIBITS\_33

record	uuid	QF3r1	Code
4087	9sp0wcxvy5719n2e	very good and goole browising is very satisfaid	1
3183	wzbf9h3cchby64yp	very good much	1
942	ey4xkq3mz2sm5k3	very good value	1
2061	660qeabng46rcsr4	Very impressive	1
3578	88hda5t7xe266xa5	Very innovative	1
1789	tcwthks9y3y1tjvc	Very nice	1
2870	n8hdns7dqvcuw95	very positve	1
2233	xzcpw59wub8k5gq5	Very useful for safety reasons	
2309	fagcma2vsqfptacg	Very well regarding to well think	1
1954	kva6f0r7782hmuk0	Visit adult sites nd third website	1
3705	jh946jk16xbjbrab	Well	1
3114	6mxuz5w4m68yn4bd	what search won't be visible to google only go the website.	2
3444	cr0ekg25nzunb2s1	when i am using in private mode, my ISP can't trace my internet usage.	
3392	chckw34yy36fqb0v	Yeah I was definitely	1
4188	zw4tqaf77mhfftry	Yes I am aware of Google Chrome lawsuit but I don't trust Google	
2725	17ga3pptwj18c5z	Yes I thought I read something recently with a company and it's employee doing illegal things under secret browsing mode.	
3030	uj63xcde3mpq5fdg	yes i usually use private mode browse i find it more security for my data and i like it more	
1394	k3h8dx8tju8y1vbu	Yes I'm going to get my lawsuit to my browsing and i loke this regarding private and i like this used everyday	
440	g9nnhan5zzbk3pme	yes it	1
3193	rb5ek7su0bnqgw9r	Yes lawsuits on Google chrome	
2368	x82akf94gx8x6e8u	Yes, I am very impressed with all these and all that.	1
3889	urbt820w4t94r1pb	You can go to jail for break the law online	

## **Exhibit 4—Keegan Study—Questionnaire**

Thank you for agreeing to participate in this anonymous survey. The survey is for research purposes only. Your responses will be held confidential and we are not trying to sell you anything.

The survey will take just a few minutes of your time. Before we begin, please read the following instructions:

- This survey makes use of images. If you are currently using a device that does not have image capabilities, please stop now and resume this survey when you have access to a compatible device.
- If you typically wear eyeglasses when reading information or looking at pictures or videos on your electronic device, please put them on now and wear them through the remainder of this survey.
- If you don't know the answer, don't recall, or don't have an opinion on any of the questions that follow, please feel free to select that answer when provided. We do not want you to guess at any of your answers.
- Please do not look up answers to any of the survey questions on the Internet or consult with any other persons regarding your survey answers.
- Your browser's back button will be disabled during the survey. Please use the "Next" button within the survey to advance through the questionnaire.

Do you understand and agree to follow the instructions provided above?

No

Yes

Don't know

Next >>

Which of the following age brackets contains your age on your last birthday?

Under 18

18 - 30

31 - 40

41 - 50

51 - 60

61 - 70

71 or older

Next >>

In which U.S. state do you currently reside?

Next >>



What is your gender?

Male

Female

Prefer to self-identify:


Prefer not to answer

Next >>

Please complete the CAPTCHA below.

☐

I'm not a robot

  
reCAPTCHA  
[Privacy](#) - [Terms](#)

Next >>

Which of the following Internet web browsers, if any, have you used in the last five years? Please select all that apply.

Chrome

Safari

Edge / Internet Explorer

Other

Don't know

Next >>

Some Internet web browsers offer a **private browsing mode**. Which of the following types of private browsing, if any, have you used in the last five years? Please select all that apply.

Private browsing mode in Edge / Internet Explorer ("InPrivate")

Private browsing mode in Chrome ("Incognito")

Private browsing mode in Safari ("Private Browsing Mode")

None of these

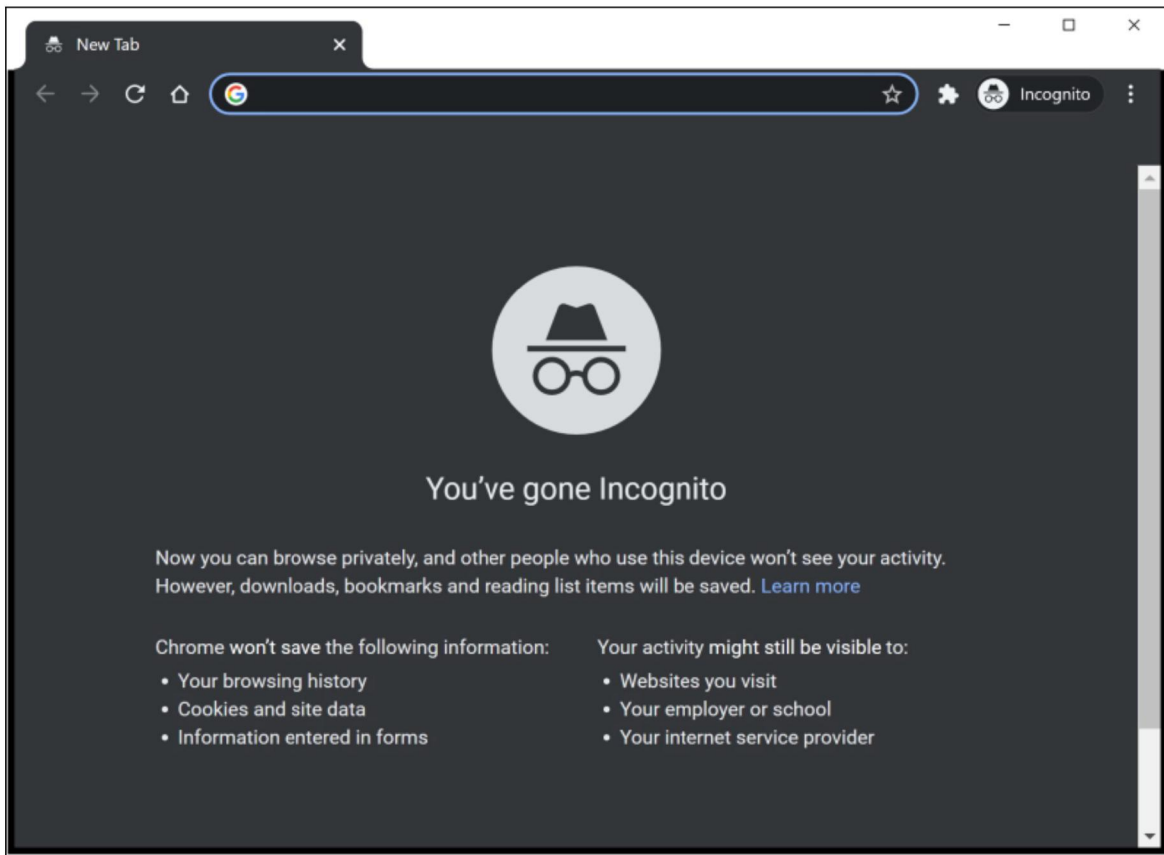
Next >>

For the remainder of this survey, if you do not know or do not have an opinion about any of the questions, please select the "don't know / no opinion" answer option. Please do not guess at any of your answers and please do not use the Internet or any other sources to inform your answers.

Click the "Next" button below to continue.

Next >>

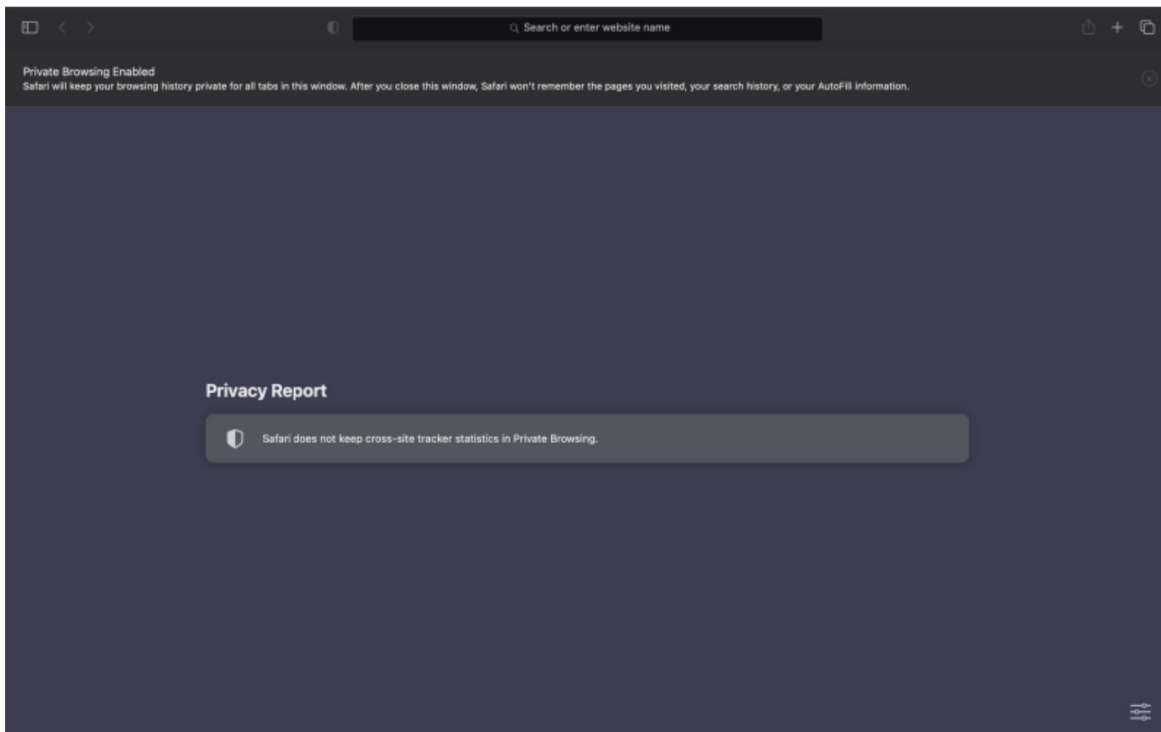
Shown below is the screen that displays when a new Chrome Incognito window is opened. Please review it as you normally would when opening a new Chrome Incognito window. You can view the image for as long as you would like. You may click on the image for an enlarged view.



Click the "Next" button below to continue.

Next >>

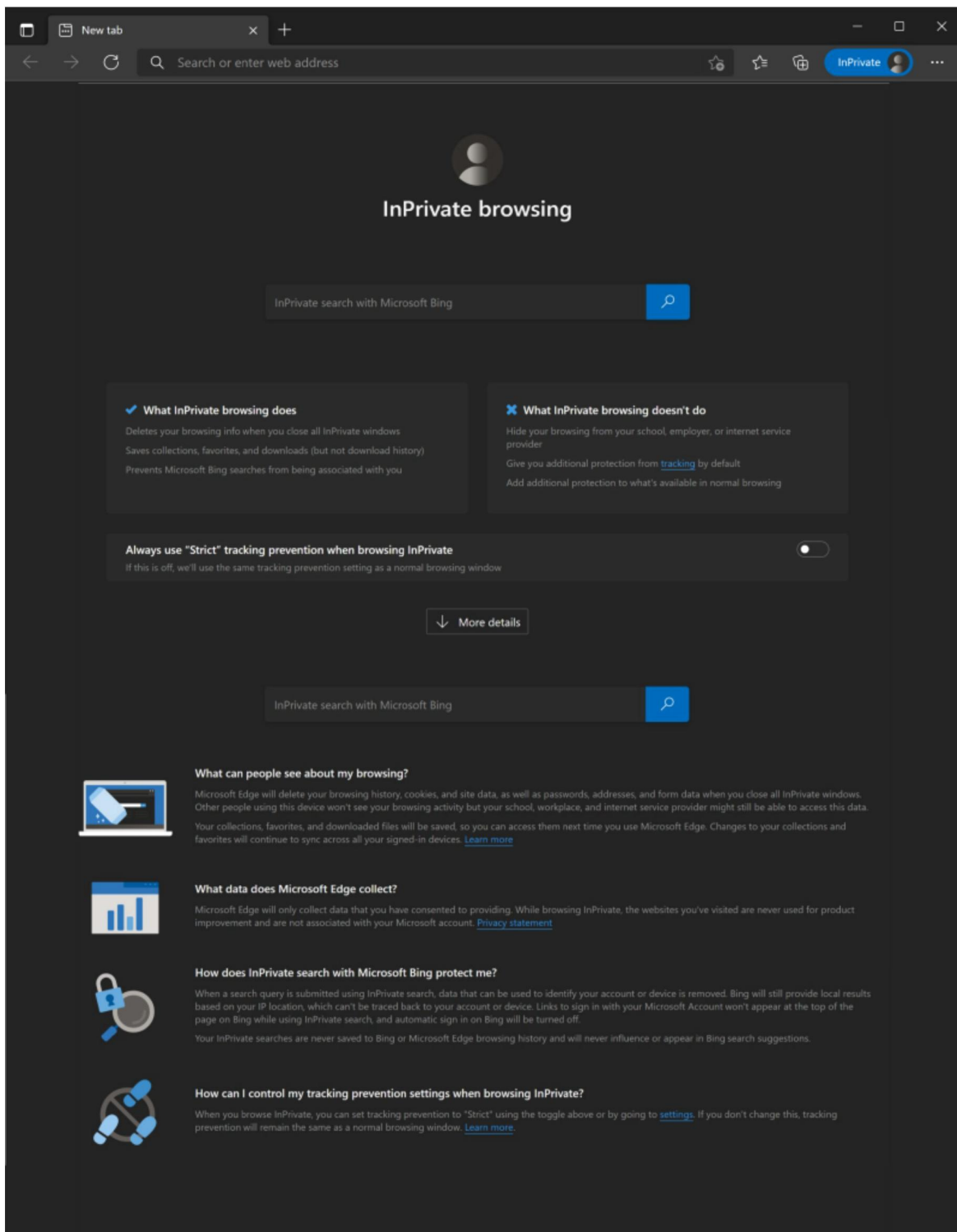
Shown below is the screen that displays when a new Safari private browsing window is opened. Please review it as you normally would when opening a new Safari private browsing window. You can view the image for as long as you would like. You may click on the image for an enlarged view.



Click the "Next" button below to continue.

Next >>

Shown below is the screen that displays when a new Edge / Internet Explorer InPrivate window is opened. Please review it as you normally would when opening a new InPrivate window. You can view the image for as long as you would like. You may click on the image for an enlarged view.



Click the "Next" button below to continue.





Please think of the time(s) that you have used private browsing mode to browse the Internet in the last five years.

Which of the following best reflects your understanding:

Google **collects and saves** my Internet browsing activity when I browse the Internet in private browsing mode

Google **does not collect and save** my Internet browsing activity when I browse the Internet in private browsing mode

Don't know / No opinion

Next >>

Please think of the time(s) that you have used private browsing mode to browse the Internet in the last five years.

Which of the following best reflects your beliefs about the level of consent that you provide Google to collect information about your Internet browsing activity when in private browsing mode?

I believe that when I am in private browsing mode, **I have not given consent** for Google to collect and save information about my Internet browsing activity

I believe that when I am in private browsing mode, **I have given consent** for Google to collect and save information about my Internet browsing activity

Don't know / No opinion

Next >>

Which of the following best reflects your opinion?

*I believe that when I am in private browsing mode, I have given consent for Google to collect and save information about my Internet browsing activity (please select all that apply):*

When I am visiting a **non-Google website**

When I am visiting a **Google website**

Don't know

Next >>

If you know, which of the following types of accounts have you had at any time during the last five years? Please select all that apply.

Google account (e.g., Gmail, Google Docs, Google Drive, Google Photos)

Microsoft account (e.g., OneDrive, Microsoft Teams, OneNote)

Apple account (e.g., iCloud, Apple Pay, Apple Music)

None of these

Next >>

Which of the following best reflects your opinion?

*I believe that when I am in private browsing mode, I have given consent for Google to collect and save information about my Internet browsing activity (please select all that apply):*

When I am **signed in** to my Google account

When I am **signed out** of my Google account

Don't know

Next >>

Please think of the time(s) that you have used private browsing mode to browse the Internet in the last five years.

Would you or would you not expect Google to collect and save each of the following types of information about your Internet browsing behavior during your private browsing mode session?

	Yes, Google would collect and save	No, Google would not collect and save	Don't know
Your IP address	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
HTTP information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cookies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your unique user ID	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your user agent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
URL information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your geolocation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your browsing activity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Next >>

Please select "Green" from the list below.

Red

Green

Yellow

Blue

Next >>



Now, a few more questions for classification purposes only. Which of the following best describes your educational background?

Less than high school

High school graduate

Some college

2-year degree

4-year degree

Master's / Professional degree

Doctorate

Next >>

Which of the following includes your household's approximate annual income in 2021?

Under \$35,000

\$35,000 - \$49,999

\$50,000 - \$74,999

\$75,000 - \$99,999

\$100,000 - \$124,999

\$125,000 - \$149,999

\$150,000 or more

I prefer not to answer

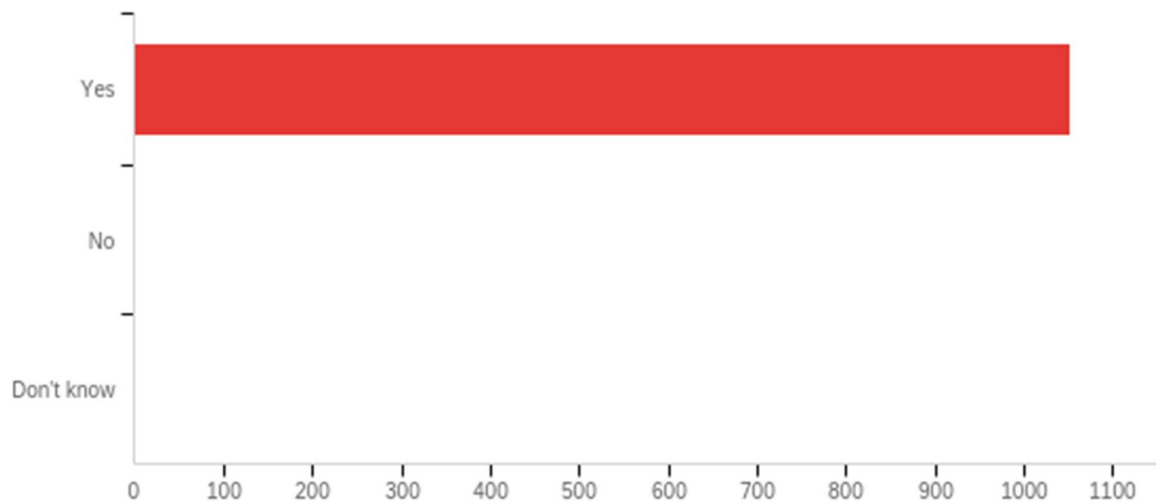
Next >>

We thank you for your time spent taking this survey.  
Your response has been recorded.

## **Exhibit 5—Keegan Study—Tabulated Data**

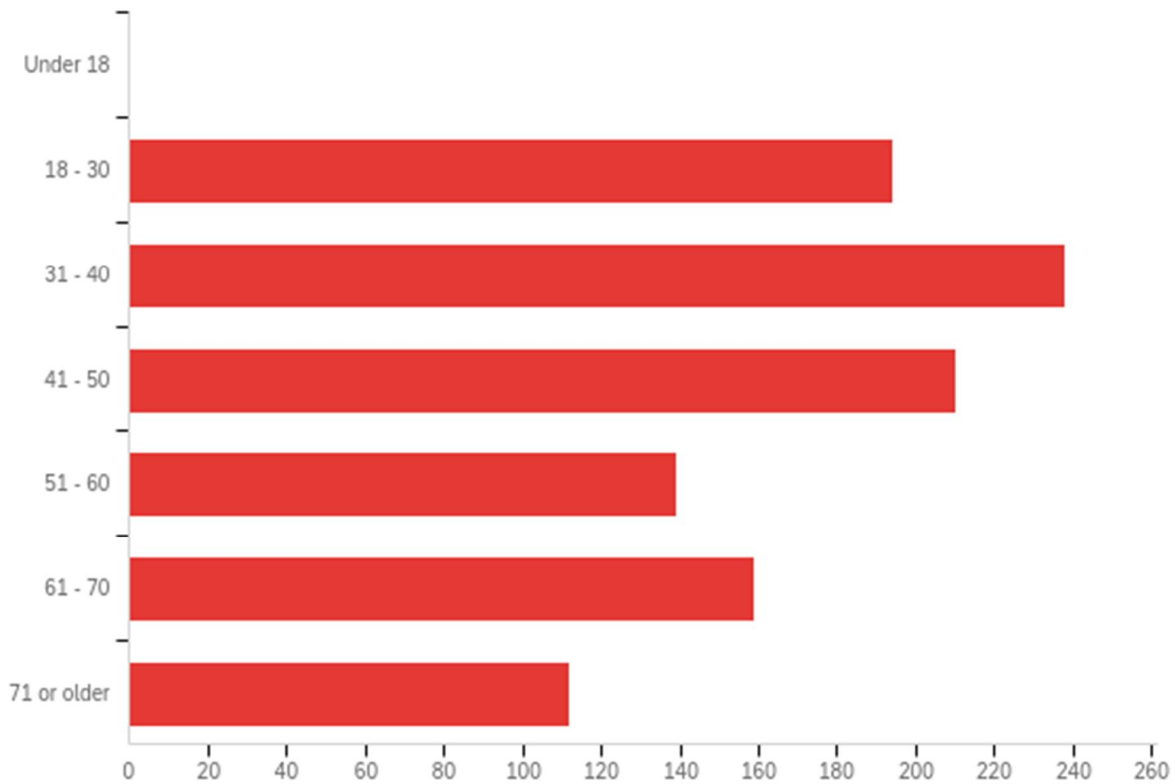
# Tabulated Data

Q1 - Beginning instruction



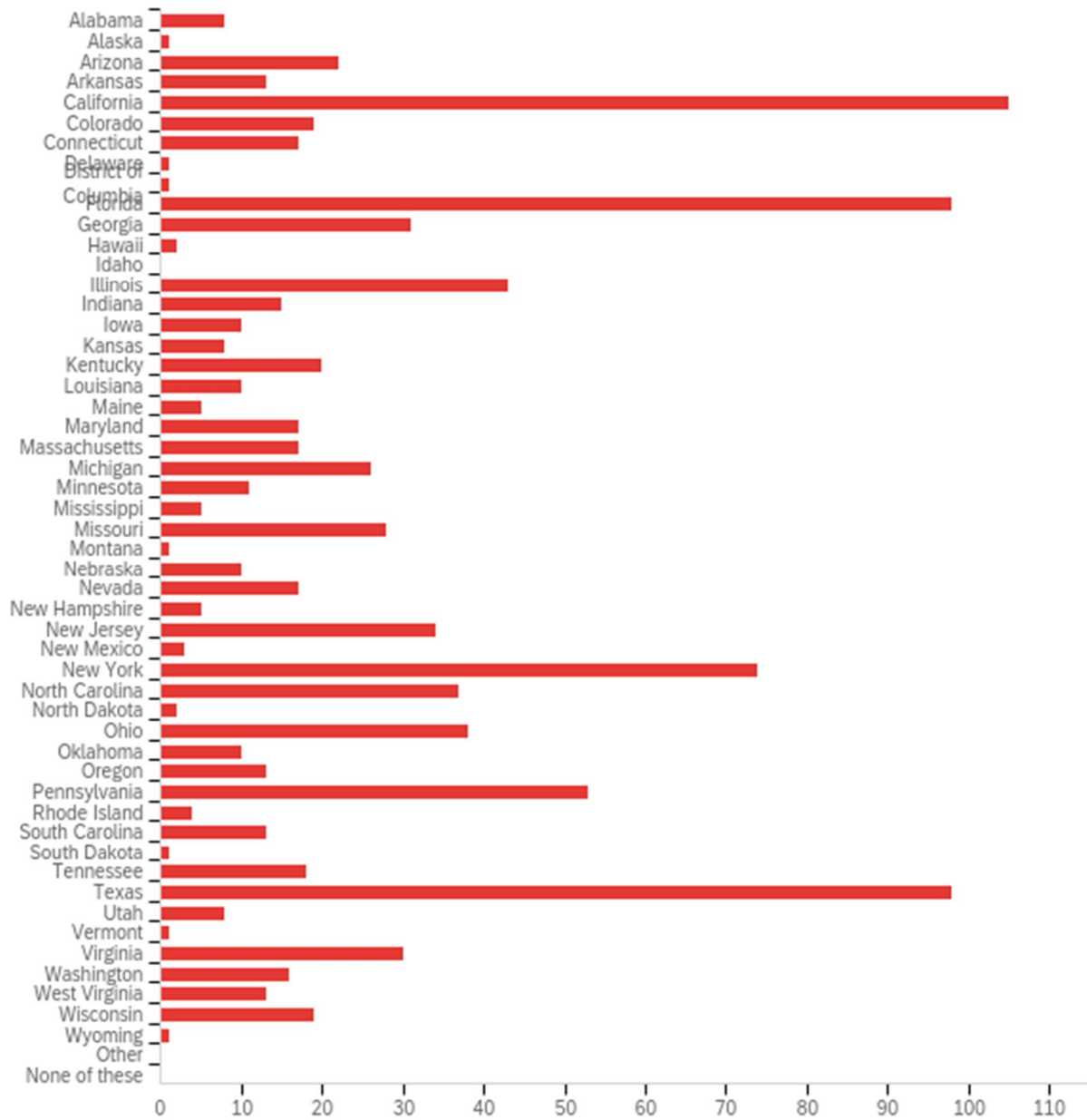
Answer	%	Count
Yes	100.0%	1052
No	0.0%	0
Don't know	0.0%	0
Total	100%	1052

## Q2 - Age



Answer	%	Count
Under 18	0.0%	0
18 - 30	18.4%	194
31 - 40	22.6%	238
41 - 50	20.0%	210
51 - 60	13.2%	139
61 - 70	15.1%	159
71 or older	10.6%	112
Total	100%	1052

## Q3 - State



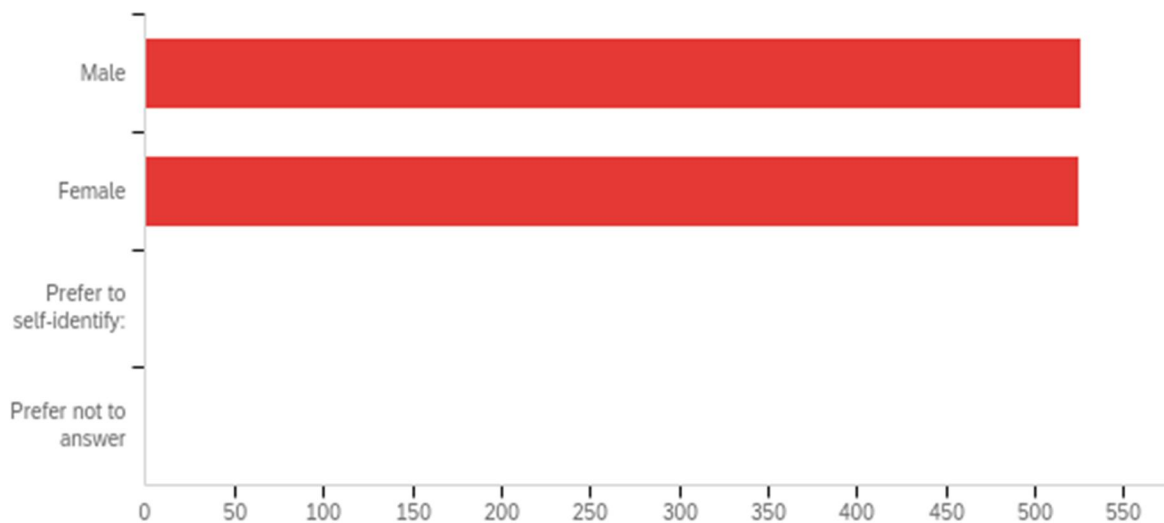
Answer	%	Count
Alabama	0.8%	8
Alaska	0.1%	1
Arizona	2.1%	22
Arkansas	1.2%	13
California	10.0%	105

Colorado	1.8%	19
Connecticut	1.6%	17
Delaware	0.1%	1
District of Columbia	0.1%	1
Florida	9.3%	98
Georgia	2.9%	31
Hawaii	0.2%	2
Idaho	0.0%	0
Illinois	4.1%	43
Indiana	1.4%	15
Iowa	1.0%	10
Kansas	0.8%	8
Kentucky	1.9%	20
Louisiana	1.0%	10
Maine	0.5%	5
Maryland	1.6%	17
Massachusetts	1.6%	17
Michigan	2.5%	26
Minnesota	1.0%	11
Mississippi	0.5%	5
Missouri	2.7%	28
Montana	0.1%	1
Nebraska	1.0%	10
Nevada	1.6%	17
New Hampshire	0.5%	5
New Jersey	3.2%	34
New Mexico	0.3%	3
New York	7.0%	74
North Carolina	3.5%	37
North Dakota	0.2%	2



Ohio	3.6%	38
Oklahoma	1.0%	10
Oregon	1.2%	13
Pennsylvania	5.0%	53
Rhode Island	0.4%	4
South Carolina	1.2%	13
South Dakota	0.1%	1
Tennessee	1.7%	18
Texas	9.3%	98
Utah	0.8%	8
Vermont	0.1%	1
Virginia	2.9%	30
Washington	1.5%	16
West Virginia	1.2%	13
Wisconsin	1.8%	19
Wyoming	0.1%	1
Other	0.0%	0
None of these	0.0%	0
Total	100%	1052

## Q4 - Gender



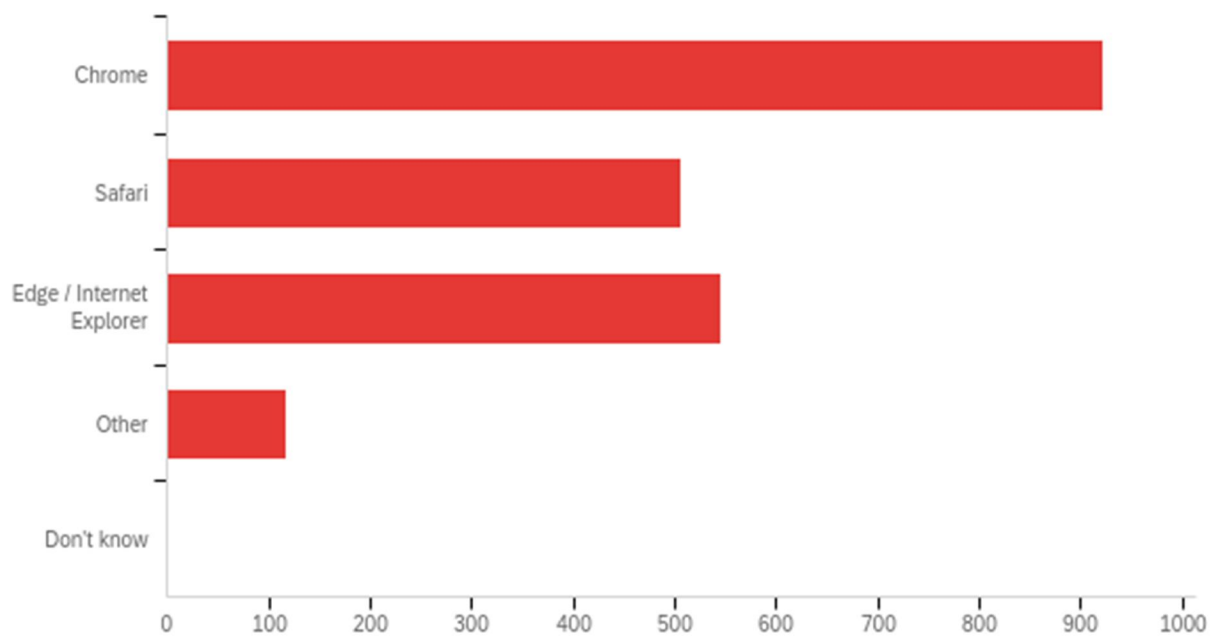
Answer	%	Count
Male	50.0%	526
Female	49.9%	525
Prefer to self-identify:	0.1%	1
Prefer not to answer	0.0%	0
Total	100%	1052

## Q4\_3\_TEXT - Prefer to self-identify:

Prefer to self-identify: - Text

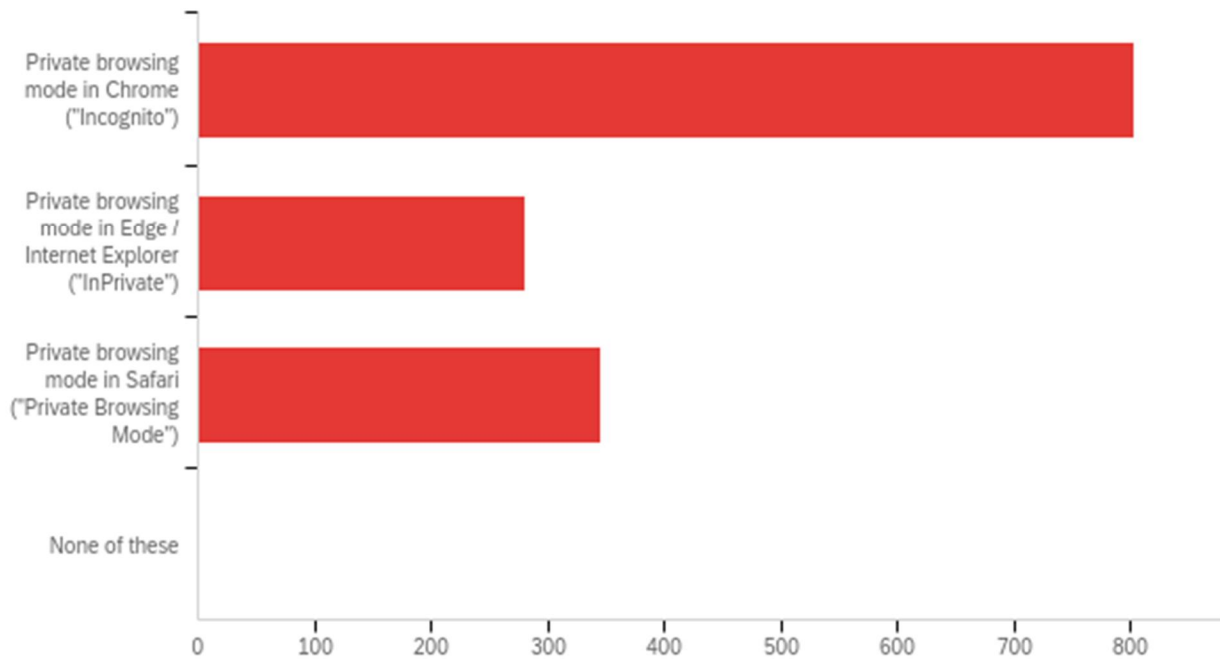
Non binary

## Q6 - Browsers



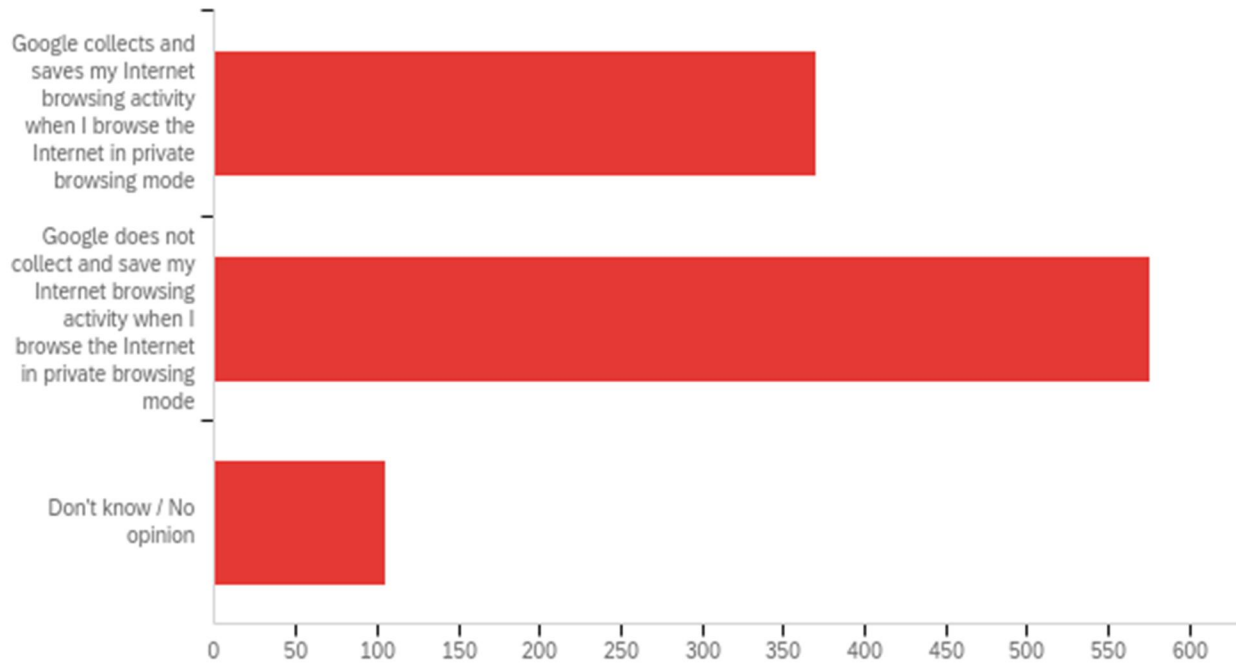
Answer	%	Count
Chrome	87.6%	922
Safari	48.1%	506
Edge / Internet Explorer	51.8%	545
Other	11.1%	117
Don't know	0.0%	0
Total	100%	1052

## Q7 - Private browsing



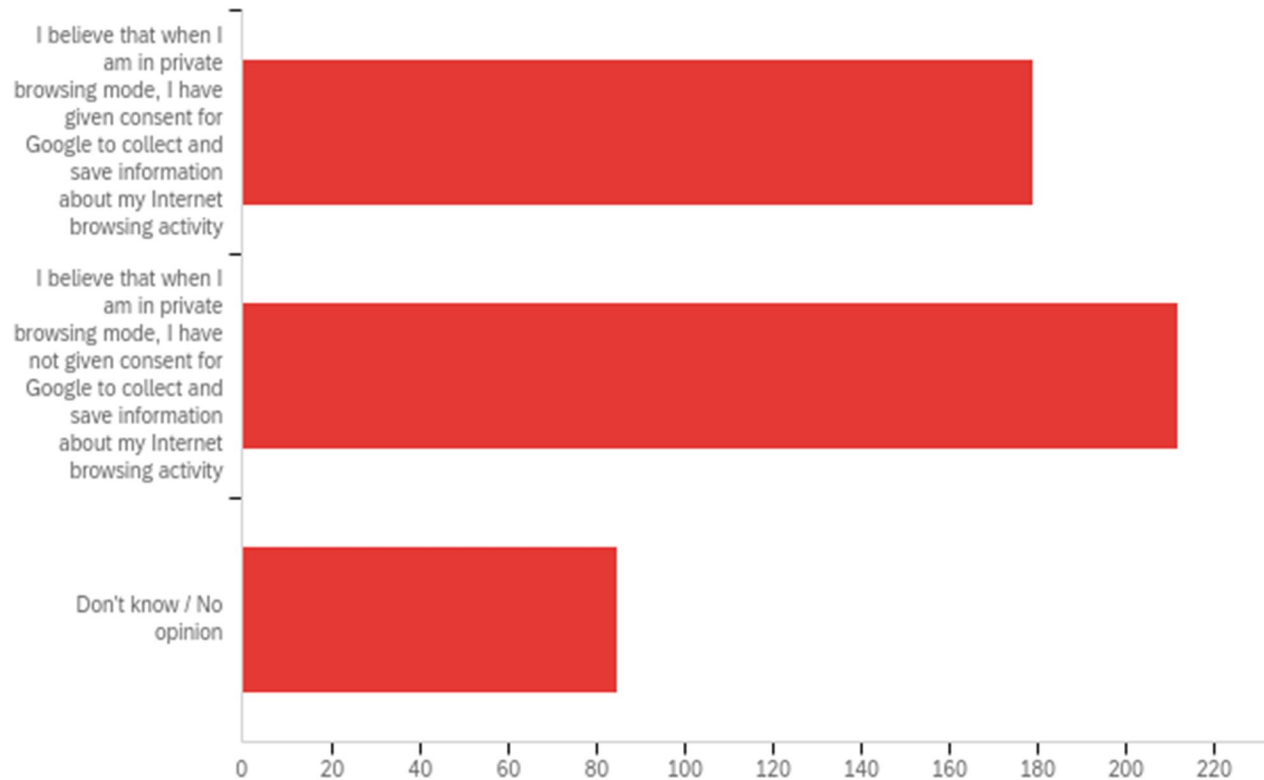
Answer	%	Count
Private browsing mode in Chrome ("Incognito")	76.3%	803
Private browsing mode in Edge / Internet Explorer ("InPrivate")	26.6%	280
Private browsing mode in Safari ("Private Browsing Mode")	32.9%	346
None of these	0.0%	0
Total	100%	1052

## Q15 - Collects and saves



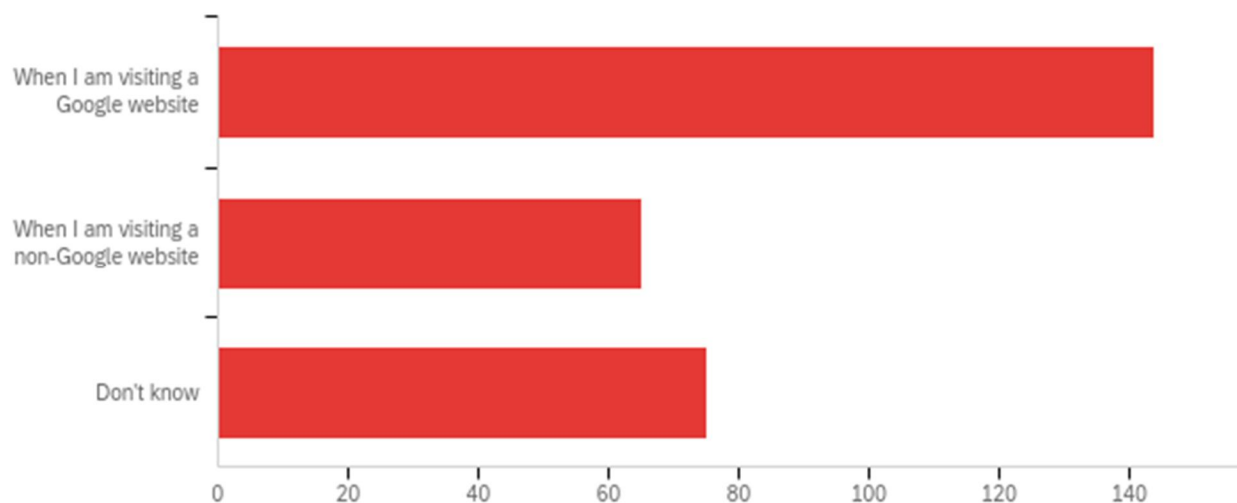
Answer	%	Count
Google collects and saves my Internet browsing activity when I browse the Internet in private browsing mode	35.3%	371
Google does not collect and save my Internet browsing activity when I browse the Internet in private browsing mode	54.8%	576
Don't know / No opinion	10.0%	105
Total	100%	1052

## Q16 - Consent



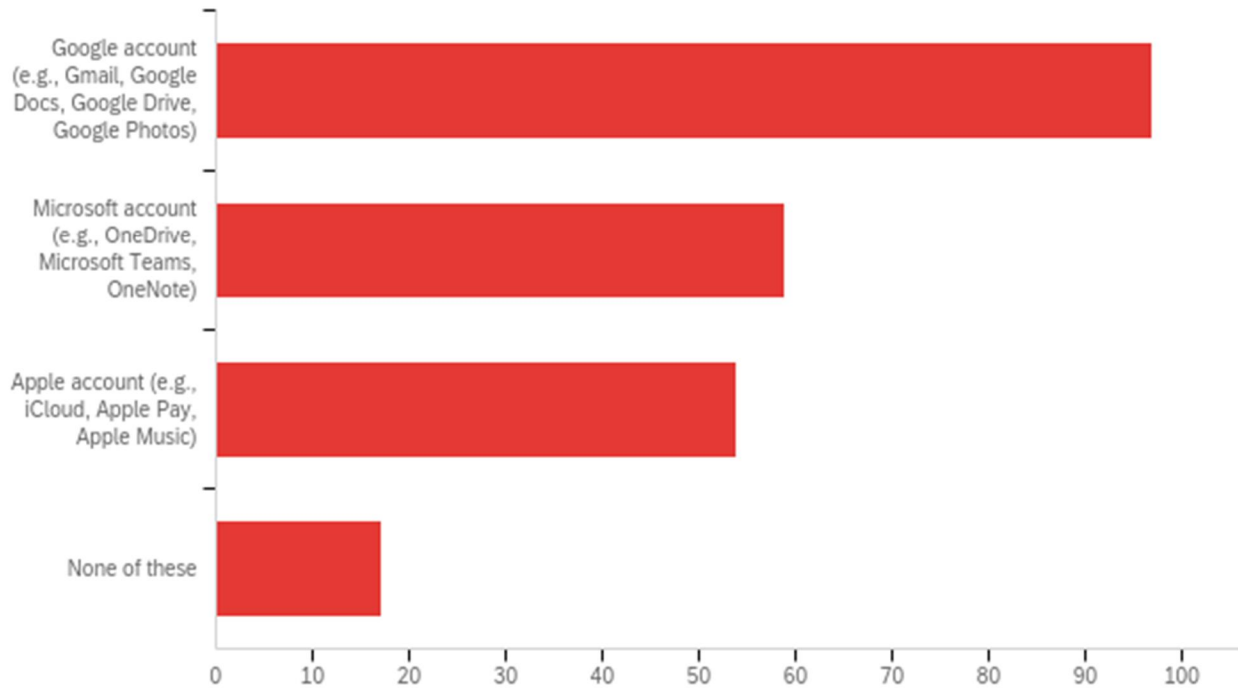
Answer	%	Count
I believe that when I am in private browsing mode, I have given consent for Google to collect and save information about my Internet browsing activity	37.6%	179
I believe that when I am in private browsing mode, I have not given consent for Google to collect and save information about my Internet browsing activity	44.5%	212
Don't know / No opinion	17.9%	85
Total	100%	476

## Q17 - Consent - Google/non-Google



Answer	%	Count
When I am visiting a Google website	54.5%	144
When I am visiting a non-Google website	24.6%	65
Don't know	28.4%	75
Total	100%	264

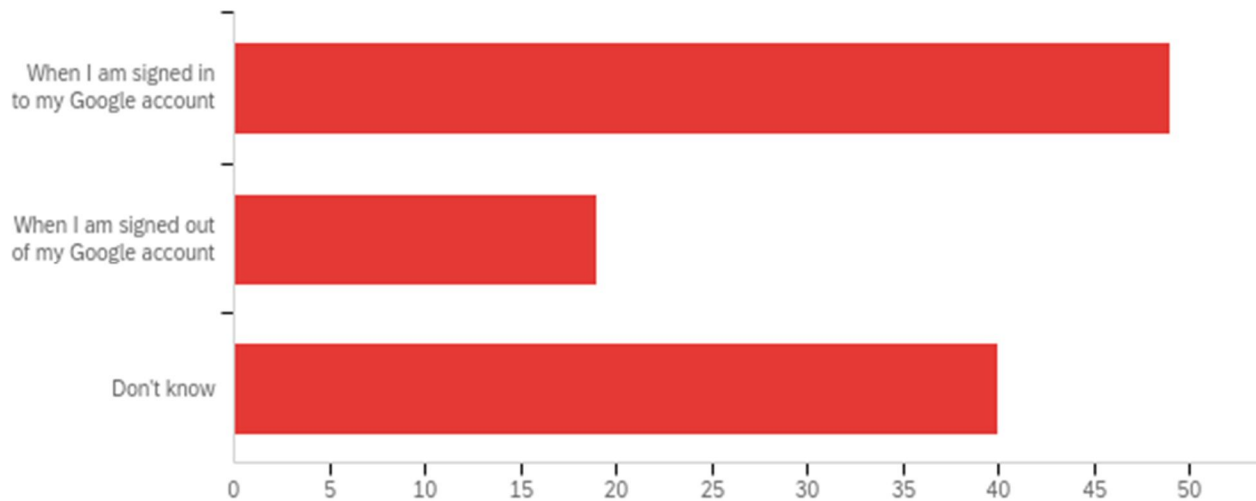
## Q18 - Accounts



Answer	%	Count
Google account (e.g., Gmail, Google Docs, Google Drive, Google Photos)	69.3%	97
Microsoft account (e.g., OneDrive, Microsoft Teams, OneNote)	42.1%	59
Apple account (e.g., iCloud, Apple Pay, Apple Music)	38.6%	54
None of these	12.1%	17
Total	100%	140

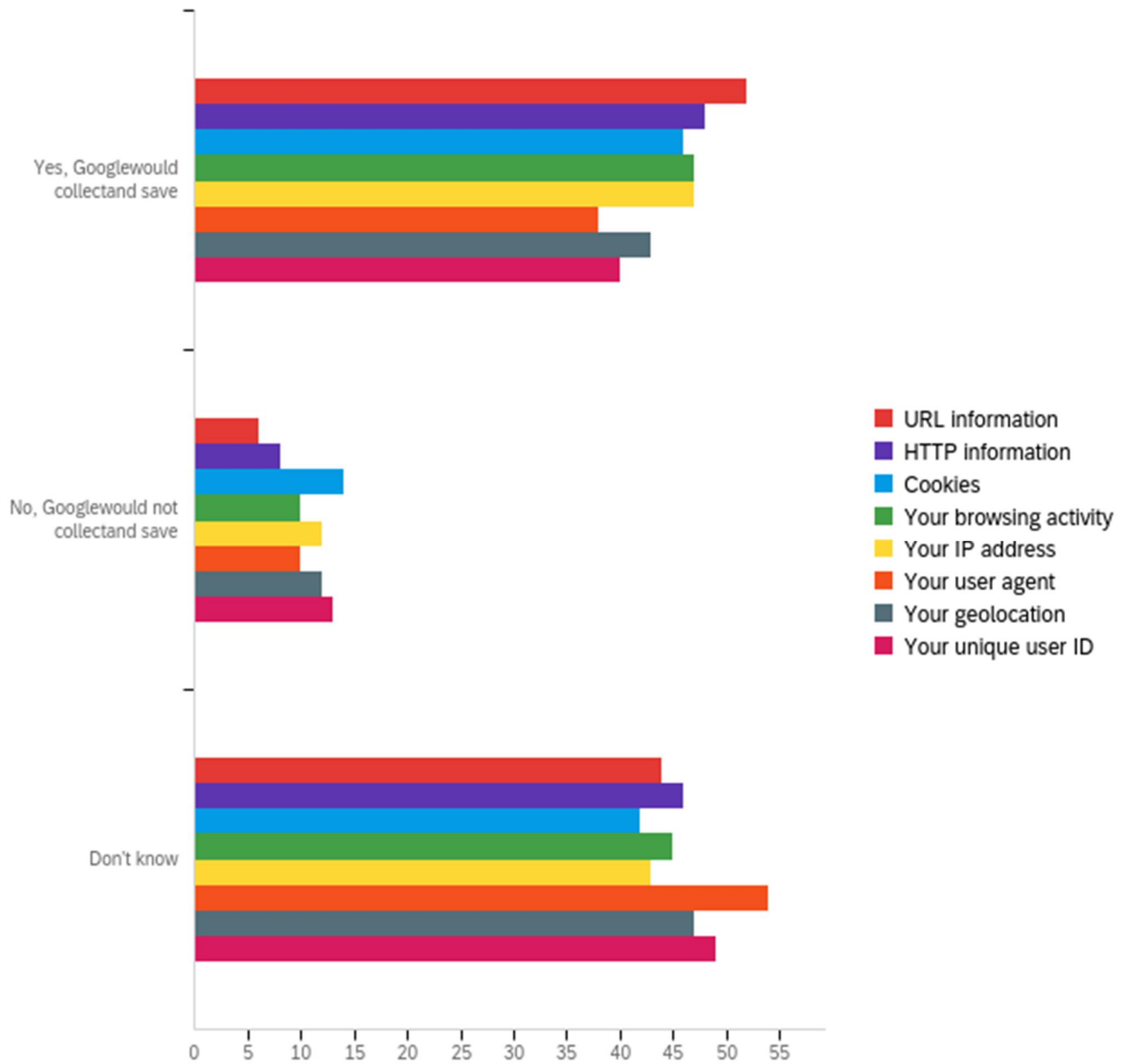


## Q19 - Consent - Signed In or Out



Answer	%	Count
When I am signed in to my Google account	50.5%	49
When I am signed out of my Google account	19.6%	19
Don't know	41.2%	40
Total	100%	97

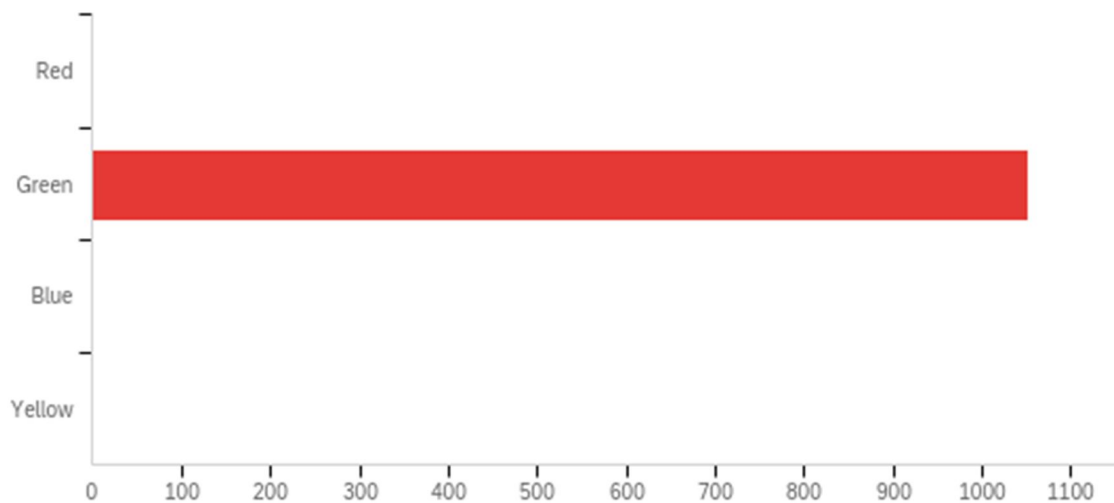
## Q20 - Matrix



Question	Yes, Google would collect and save		No, Google would not collect and save			Don't know		Total
URL information	51.0%	52	5.9%	6		43.1%	44	102
HTTP information	47.1%	48	7.8%	8		45.1%	46	102
Cookies	45.1%	46	13.7%	14		41.2%	42	102
Your browsing activity	46.1%	47	9.8%	10		44.1%	45	102
Your IP address	46.1%	47	11.8%	12		42.2%	43	102

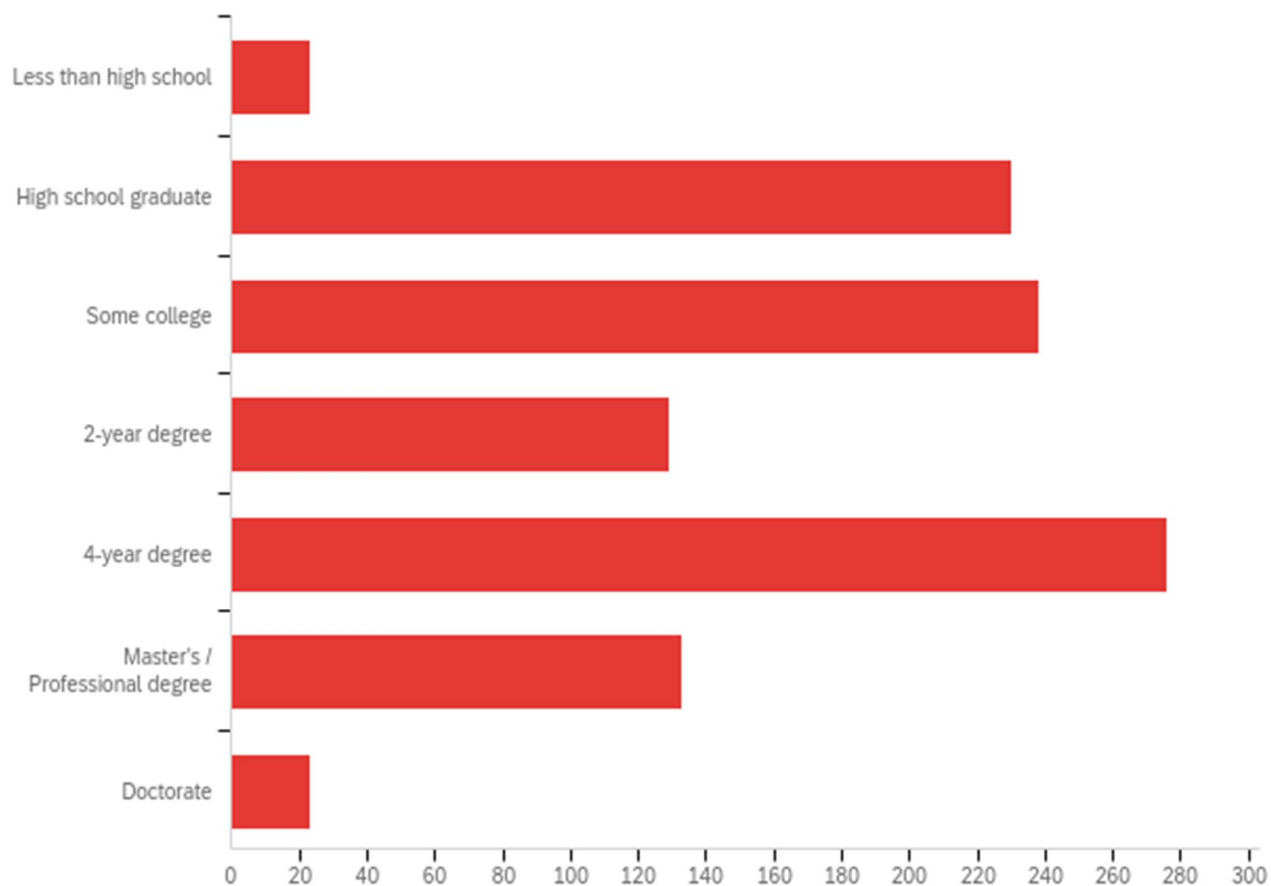
Your user agent	37.3%	38	9.8%	10	52.9%	54	102
Your geolocation	42.2%	43	11.8%	12	46.1%	47	102
Your unique user ID	39.2%	40	12.7%	13	48.0%	49	102

## Q21 - Green



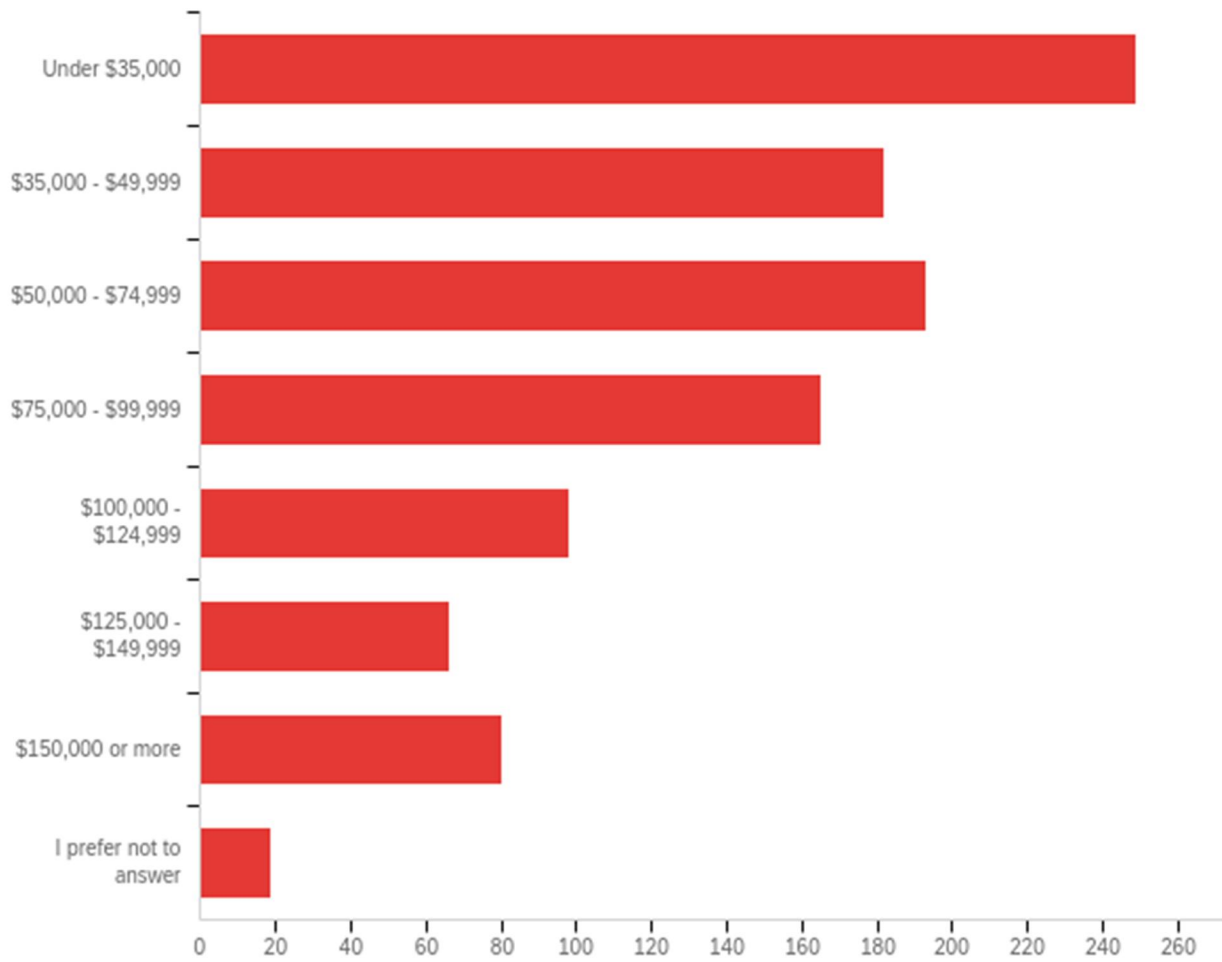
Answer	%	Count
Red	0.0%	0
Green	100.0%	1052
Blue	0.0%	0
Yellow	0.0%	0
Total	100%	1052

## Q22 - Education



Answer	%	Count
Less than high school	2.2%	23
High school graduate	21.9%	230
Some college	22.6%	238
2-year degree	12.3%	129
4-year degree	26.2%	276
Master's / Professional degree	12.6%	133
Doctorate	2.2%	23
Total	100%	1052

## Q23 - Income



Answer	%	Count
Under \$35,000	23.7%	249
\$35,000 - \$49,999	17.3%	182
\$50,000 - \$74,999	18.3%	193
\$75,000 - \$99,999	15.7%	165
\$100,000 - \$124,999	9.3%	98
\$125,000 - \$149,999	6.3%	66
\$150,000 or more	7.6%	80
I prefer not to answer	1.8%	19
Total	100%	1052

## **Exhibit 6—Keegan Study—Untabulated Data**

Produced electronically.

## **Exhibit 7—Keegan Study—Disposition of Contacts**

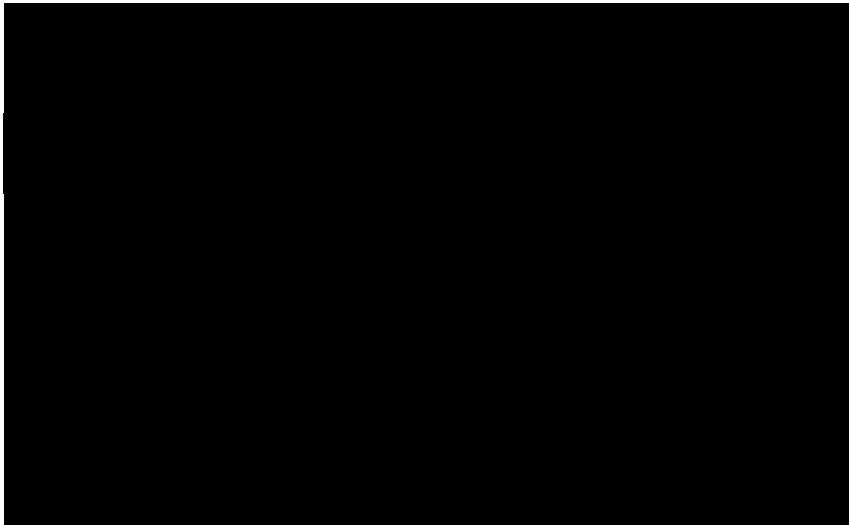




#### Disposition of Contacts - Chasom Brown, et al. v. Google LLC

	n	%
Responded to invitation	1,987	100.0%
Rejected - failed instruction acknowledgement question	111	5.6%
Rejected - failed age question (under 18)	11	0.6%
Rejected - failed - state (selected "other" or "don't know")	2	0.1%
Rejected - failed - not a Chrome, Safari, or Edge/IE user	82	4.1%
Rejected - failed - not a Chrome, Safari, or Edge/IE private browsing user	708	35.6%
Rejected - failed security question ("Green")	3	0.2%
Rejected - speeder	1	0.1%
Rejected - over quota	17	0.9%
Total qualified respondents	1,052	52.9%

## **Exhibit 8—Summary of Google Internal Documents**

Production Number	Description
GOOG-BRWN-00228597	On June 12, 2008, a Google employee sent email referencing interviews of Google employees (“non-eng Googlers”) regarding Incognito, noting a participant had “[p]rivacy concerns” and asked “if go incognito is REALLY going incognito[.]”
GOOG-BRWN-00477487	On July 10, 2008, a Google employee circulated “feedback from the UX [user experience] studies” (at -487), where “most users did not fully understand what ‘Go Incognito’ was from the name alone” (at -488), noting that “a common misconception is that ‘go incognito’ will stop the server storing information” (at -488) and a “server logging misunderstanding” (at -489).
GOOG-BRWN-00409986	On July 17, 2008, a Google employee circulated “Chrome team meeting notes” (at -986) reporting that “People didn’t understand Incognito. Does it keep sites from logging stuff on their servers? (at -987).”
GOOG-BRWN-00477510	 at -513-514).
GOOG-BRWN-00812091	In March 2014, a Google employee wrote that “The spy imagery is absolutely NOT what we want to keep portraying. It’s unfortunate that we already have it. Incognito does NOT support the kinds of guarantees that people imagine for a ‘spy mode.’”
GOOG-CABR-05287675	On September 23, 2014, a Google employee sent an email stating that “people don’t and indeed cannot understand Incognito’s guarantee(s) and non-guarantee(s),” that “[n]ormal people have no chance,” and that “Incognito’s confusability is actively harmful to the Chrome and Google brands.”
GOOG-BRWN-00457255	On September 25, 2014, a Google employee sent an email stating that Chrome Incognito users were “operating under a false sense

Production Number	Description
	of privacy” and that there is a need for Google to make changes so “we don’t deceive users.”
GOOG-BRWN-00806482	In January 2015, Google employees discussed issues with people “perceiv[ing] that Incognito provides a guarantee of unlinkability” and noting that “[p]erception is the entire problem, and we foolishly fan the flames.”
GOOG-CABR-05370279	In January 8, 2015, a Google employee stated that “the fault lies partly with the name and the iconography” where “we give things names and icons that promise things that the software is not delivering.”
GOOG-BRWN-00630517	In February 2015, a Google employee described Incognito as “radioactive” and “effectively a lie.”
GOOG-CABR-00111856	An August 2015 document named “Exploration of primary value proposition of Incognito to users - GCS” notes that “[p]revious <u>survey</u> showed that there are various misconceptions among users on what an Incognito browser provides in terms of protecting their privacy,” and that “[b]ased on this research, we hypothesized that Chrome’s Incognito may benefit from a re-design of its tab page such that its true functionality and model of operation is more accurately conveyed” (at -856).
GOOG-BRWN-00390418	In an April 2016 email, Google employee Sabine Borsay lamented “how much we’re actually struggling with the Incognito branding and misconceptions it causes,” including after “[a]ll the years of research.”
GOOG-CABR-00353831	In May 2016, a Google employee expressed that “it’s extremely disappointing that ‘Incognito’ was used for another prominent Google feature that, unlike Chrome’s Incognito, offers e2e encryption. I expect it will lead to confusion” (-831).
GOOG-CABR-04971904	Discussing Incognito in May 2016, a Google engineer lamented: “This isn’t just marketing, it isn’t just a word, this isn’t OK. This is a problem of professional ethics and basic honesty, and if we want to call ourselves security engineers and privacy engineers, we need to fix it.” (at -04).
GOOG-BRWN-00410884	On June 21, 2016, a Google employee sent an email concerning “Google ‘Incognito’ Precision” stating that “nothing will be more scannable than the name and the icon, both of which are a poor fit for what the feature actually provides” (at -884).
GOOG-BRWN-00475063	In July 2018, a Google employee wrote that he “kn[e]w the ‘incognito war was waged and lost years ago, but do you know why? It has always been a misleading name” (at -065). Another

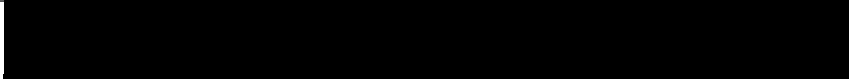
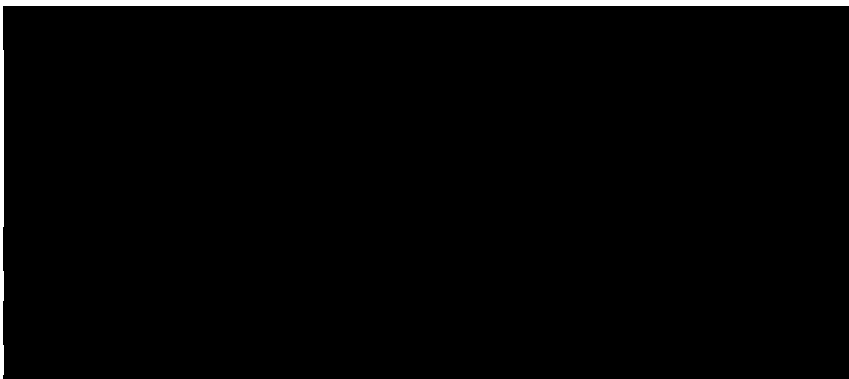
Production Number	Description
	Google employee wrote “we need to stop calling it Incognito and stop using a Spy Guy icon” (at -065).
GOOG-CABR-04718352	A document called “Five ways people misunderstand Incognito and private browsing” authored by Google employee Martin Shelton reports that “Private browsing has a problem. In both internal and external research, we’ve seen that the privacy properties of Incognito aren’t well understood, to say the least. And the same is true for all modern browsers with a private browsing mode” (at -352). Mr. Shelton lists “common misconceptions,” including that “[m]ost users believe their private browsing activity won’t be remembered by Google, even after they sign into their account” ( <i>id.</i> ). He notes that “[t]hese misconceptions could give users a false impression of privacy in a moment when they expect it most, leading them to inadvertently share sensitive personal data,” and proposes Google “be bolder about saying <i>who sees what</i> as we browse the web,” beginning with making “creative changes to naming conventions, iconography, explanation strings, and/or the function of Incognito itself” ( <i>id.</i> ).
GOOG-BRWN-00140297	A July 2018 Google presentation called “The Incognito Problem” reported that “[w]e know from intuition, anecdotes, and now empirically (Yuxi Wu, et al.; see also Habib, et al.) that the ‘incognito’/Spy Guy branding, and the complex disclosures (like all complex disclosures), confuse people as to what exact guarantees it offers and does not offer” (at -299). That Google presentation states “[w]e are over-promising and under-delivering” (at -302) and recommends to “[u]se less loaded terms and iconography” and “[s]implify the disclosure/disclaimer” (at -315).
GOOG-BRWN-00797584	On July 21, 2018, Google employee Mr. Palmer shared “The Incognito Problem” presentation with other Google employees, including the Google “Chrome Privacy Core” listserv and the Google [REDACTED] listserv.
GOOG-BRWN-00634444	In July 2018, regarding “The Incognito Problem,” Google employee Dr. Adrienne Porter Felt stated she was a “fan” of “dial[ing] up Incognito to get closer to users’ expectations.”
GOOG-CABR-00084985	In July 2018, Google admitted in an internal presentation that users experienced “several common misconceptions” about “how Incognito works” and admitted that “[t]he same is true for private browsing more generally.” (at -043)
GOOG-BRWN-00804212	On August 22, 2018, Google employee Mr. Palmer asked Dr. Porter Felt for her “views, if any, on The Incognito Problem? (Or do you agree there is a problem?)” and Dr. Porter Felt responded she “agree[s] there is an incognito problem.”

Production Number	Description
GOOG-BRWN-00042339	An August 2018 Google presentation called “How Do Users Interpret Alternative Incognito Metaphors” describes a survey of active Chrome users to assess a possible change to the Chrome Incognito icon, asking participants “whether they believe their search history would be remembered when they logged into Google” (at -341). Summarized findings include: “Most Chrome users do not understand what is and is not saved when logging into an account in Incognito, even if they are experienced using it” (at -347).
GOOG-CABR-03764749	In August 2018, Martin Shelton, a User Experience Researcher at Google, explained that the words “Incognito” and “private” are problematic insofar as they reinforce the “misperception that your browsing is private <i>everywhere</i> instead of just on your device” (at -50)
GOOG-BRWN-00047390	A September 24, 2018 Google document called “Incognito Mode, Current and Possible Promises” includes a section on “[r]educing user confusion” notes that [REDACTED] (at -397).
GOOG-CABR-04261880	On September 24, 2018, a Google employee stated that Incognito “misconceptions flow directly from the framing of the feature as ‘Incognito’ (or, for other browsers, ‘Private’).”
GOOG-CABR-03923580	On November 5, 2018, a Google employee stated that “the blame for people’s misconceptions about Incognito mode is due to that name and branding,” as that employee “had argued repeatedly” (at -581).
GOOG-CABR-00094550	A Google document created in 2019 noted that “[r]esearch indicates that most users do not currently understand the current messaging” of Incognito mode and proposed changes to the Incognito Splash Screen to use “simple iconography” to “explain simply to a user who they are protected from,” including to explain if “[y]ou are protected from Google.”
GOOG-BRWN-00848723	A January 2019 Google presentation includes “UXR Questions” (at -724). In response to the question “Do users really understand what they’re consenting to when they consent to share browsing history or other behaviour data,” the presentation states: “No. The research shows that participants don’t read the text without guidance and don’t understand the text when they do” and also that “a large fractions of users feel they have no choice in the bargain, or that the choice is difficult to find and the playfield is slanted against them” (at -726).

Production Number	Description
GOOG-CABR-04991831	On February 27, 2019, Google employee sent an email discussing [REDACTED] plans” and an “upcoming exec review” with Google CEO Sundar Pichai, where topics included “[e]nhancements to Incognito, in line with the thinking from Chris Palmer and others.”
GOOG-CABR-00142741	A March 2019 Google presentation called “User Needs & Misconceptions” includes a set of slides labeled “Common Misconceptions” (at -745) referencing the March 2018 “Five misconceptions of Incognito Mode” (at -746) discussed above. The presentation acknowledges that the “idea that incognito can provide anonymity creates a false sense of security in returning incognito users” and notes that “user perceptions around these [Incognito] protections tend to be focused at the level of the webpage,” not just the level of the device (at -747). The presentation also describes how Google uses the Incognito brand in other products despite “[i]nconsistencies mak[ing] it difficult for users to develop a consistent mental model” (at -751).
GOOG-BRWN-00047341	In a December 2019 internal Google presentation, Google discussed the need to [REDACTED] (at -44).
GOOG-CABR-00141578	A January 2020 Google document “[r]ecommend[ing] [a] position for Chrome” reported that “[r]esearch strongly suggests that a significant proportion of users already expect Incognito to protect them from tracking on the network-stack and from the web-server” (at -579).
GOOG-CABR-05148261	In a January 2020 internal Google presentation, Google admitted that “When Incognito is on,” Google should not “save IP addresses or other unique IDs.” (at -73).
GOOG-BRWN-00042388	A March 2020 Google presentation called “Incognito Mode UXR Review” includes a section called “Misconceptions & Expectations” (at -402) (with references to “sumUX Research March 2020” and “Chrome Lit. Review 2018” studies) reports that participants in those studies “do not understand how private mode works” and “overestimate private mode protections” (-403). It lists “several common misconceptions about private mode, including that it prevents all external parties from accessing user data and search history, safeguards against hacking, and protects against tracking and ad targeting... gives anonymity, obscures location, hides browsing activity from Google” (at -403). It also notes that





Production Number	Description
	 ” (at -842).
GOOG-CABR-04668451	A July 14, 2021 email with the subject “Incognito NTP Revamp” notes “User problem: Users have misconceptions about Incognito and often overestimate the protections available.”
GOOG-CABR-04746153	 ” (at -172).

# **EXHIBIT 80**

## **6/7/2022 EXPERT REBUTTAL REPORT OF GEORGIOS ZERVAS, PHD**

**Redacted Version of  
Document Sought to  
be Sealed**

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**UNITED STATES DISTRICT COURT**  
**NORTHERN DISTRICT OF CALIFORNIA, OAKLAND DIVISION**

CHASOM BROWN, WILLIAM BYATT,  
JEREMY DAVIS, CHRISTOPHER  
CASTILLO, and MONIQUE TRUJILLO,  
individually and on behalf of all other  
similarly situated,

Plaintiff,

v.

GOOGLE LLC,  
Defendants.

Case No. 5:20-cv-03664-YGR

**EXPERT REBUTTAL REPORT OF GEORGIOS ZERVAS, PHD**

**JUNE 7, 2022**

**TABLE OF CONTENTS**

I.	EXECUTIVE SUMMARY .....	1
II.	INTRODUCTION .....	14
A.	Qualifications .....	14
B.	Assignment .....	15
C.	Facts And Data Considered .....	16
III.	REBUTTAL TO MR. HOCHMAN’S DESCRIPTIONS OF GOOGLE’S ANALYTICS AND ADVERTISING SERVICES .....	16
A.	Mr. Hochman’s Assertions That Google “Intentionally Intercepts” Private Browsing Communications Are Inaccurate (Hochman Opinion 1) .....	16
B.	Mr. Hochman Does Not Provide Any Support For His Opinion That “Tracking Beacons” Collect The Content Of Users’ Communications (Hochman Opinion 2) .....	23
C.	Mr. Hochman Fails To Establish That Google “Copied” Information From Users’ Communications .....	24
D.	Mr. Hochman’s Assertion That Google “Tracking Beacons” “Neither Facilitate Nor Are Incidental To” Users’ Communications With Websites Is Incorrect (Hochman Opinion 3) .....	27
	1. Google’s Analytics And Advertising Services And Related Tags Facilitate And Are Incidental To Users’ Communications With Websites .....	28
	2. Importance Of Analytics Services .....	30
	3. Importance Of Advertising To Websites And Users .....	34
E.	Mr. Hochman’s Assertion That Google Could Have Designed Chrome Differently Is Speculative And Misleading (Hochman Opinion 4) .....	36
IV.	REBUTTAL TO MR. HOCHMAN’S ASSERTIONS REGARDING USER AND WEBSITE NOTIFICATIONS .....	41
A.	Mr. Hochman’s Opinions Regarding User Notification And Choice Are Flawed (Hochman Opinion 5) .....	41
B.	Mr. Hochman’s Opinions Regarding Notifications To Websites Are Flawed (Hochman Opinion 6) .....	48
V.	REBUTTAL TO MR. HOCHMAN’S ASSERTIONS REGARDING USER PROFILES (HOCHMAN OPINION 10) .....	51
VI.	REBUTTAL TO MR. HOCHMAN’S ASSERTION THAT GOOGLE CIRCUMVENTED COOKIE BLOCKERS AND ANTI-TRACKING MEASURES (HOCHMAN OPINION 15) .....	52

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

1. PPID.....	52
2. Enhanced Conversions.....	55
VII. REBUTTAL TO MR. HOCHMAN’S OPINIONS REGARDING IMPACT ON USERS (HOCHMAN OPINIONS 26 THROUGH 28).....	57
VIII. REBUTTAL TO MR. HOCHMAN’S ASSERTIONS REGARDING HOW CHROME’S INCOGNITO MODE OPERATES (HOCHMAN OPINION 29).....	60
IX. OTHER REBUTTALS TO MR. HOCHMAN’S REPORT.....	64
A. Mr. Hochman Exaggerates The Complexity Of Developer Tools .....	64
B. Mr. Hochman’s Statements About Energy Saving And Performance Of Websites Related To Google’s Analytics And Advertising Services Are Flawed.....	68
C. Mr. Hochman’s Assertion That Users Cannot Request Deletion Of Private Browsing Data Incorrectly Assumes That Google Can Identify Specific Users Associated With The Data .....	69

## I. EXECUTIVE SUMMARY

1. I have been engaged in this matter by counsel for Google LLC (“Google”) to respond to certain opinions in the Expert Report of Jonathan E. Hochman.<sup>1</sup> Specifically, I address Mr. Hochman’s Opinions 1 through 6, 10, 15, and 26 through 29 pertaining to Mr. Hochman’s description of how Google’s analytics and advertising services function and whether Private Browsing Mode functions as described in public documents.<sup>2</sup> I understand that experts Konstantinos Psounis and Paul Schwartz are submitting expert reports in which they will address other opinions in Mr. Hochman’s report. Based on my experience, the materials I reviewed in this matter, and my testing of Chrome and other browsers in my opening report, I have reached the following opinions.

### **Zervas Rebuttal Opinion 1 (See Section III.A)**

2. In my opinion, Mr. Hochman’s assertion in his Opinion 1 that “Google intentionally intercepted private browsing communications between users and non-Google websites while those communications were in transit”<sup>3</sup> and his descriptions of Google’s receipt of information as “interception” or “surveillance”<sup>4</sup> are misleading. Mr. Hochman fails to

---

<sup>1</sup> Expert Report of Jonathan E. Hochman, April 15, 2022 (“Hochman Report”).

<sup>2</sup> Throughout this report and consistent with my opening report, I use the term “Private Browsing Mode” to refer generally to private browsing modes of various browsers, and I use the term “Private Browsing Session” to refer to browsing sessions where the browser is in Private Browsing Mode. I use the term “Incognito Mode” or simply “Incognito” to refer to the Private Browsing Mode of the Chrome browser in particular. I use the term “Regular Mode” to refer to browsing modes other than Private Browsing Mode. Regular Mode can encompass multiple modes of browser operation depending, for example, on a user’s sign-in state.

<sup>3</sup> Hochman Report, Section VIII.A.

<sup>4</sup> See e.g., Hochman Report, ¶¶ 78-79, 82-84; Hochman Report, Appendix A, ¶ 17.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

acknowledge that Google receives transmissions of At-Issue Data<sup>5</sup> because website developers have decided to use one or more of Google’s services by incorporating code into their website to cause those transmissions. Mr. Hochman also fails to acknowledge that it is well known and understood in the web development industry that when a website developer uses one or more third-party services and installs the relevant code on their website to enable that functionality, it will result in transmission of certain data to those third-party services.

3. Mr. Hochman also fails to acknowledge that how Private Browsing Modes operate is widely understood in the industry. For example, the World Wide Web Consortium (“W3C”) states that browser vendors should design private browsing modes so that they work in a way that is “indistinguishable” for websites from normal browsing mode.<sup>6</sup> Mr. Hochman has not identified, and I have not seen, any evidence indicating that website developers expect that the third-party services they have chosen to use on their website, such as Google’s analytics and advertising services, will cease to function when a user visits their website in a Private Browsing Mode.

4. It is my opinion that those who are familiar with how modern websites operate and how browsers communicate with those websites, even at a general level, would not use terms like “interception” or “surveillance” to describe Google’s receipt of information related to a user’s visit in Private Browsing Mode to a website that uses Google’s analytics or advertising services.<sup>7</sup> To

---

<sup>5</sup> In my opening report, I summarized the categories of information that Plaintiffs allege Google collects and enable Google to identify users, their devices, and activity as “At-Issue Data.” See, Expert Report of Dr. Georgios Zervas, April 15, 2022 (“Zervas Affirmative Report”), ¶ 14. Mr. Hochman does not use the term At-Issue Data but instead refers to information sent to Google as “communications” and “transmissions.” For purposes of this report, I use the terms “communication” and “transmissions” to be consistent with the terminology used by Mr. Hochman.

<sup>6</sup> “W3C TAG Observations on Private Browsing Modes,” W3C, July 5, 2019, available at <https://perma.cc/5CHW-LNER>.

<sup>7</sup> See, e.g., Hochman Report, ¶¶ 78-79, 82-84; Hochman Report, Appendix A, ¶ 17.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

the contrary, Google provides its analytics and advertising services to website developers who take the active step of installing the relevant code on their websites. If the website developers do not install and enable Google’s analytics and advertising code, Google would not receive these communications. As a result, I do not agree with Mr. Hochman’s opinion that these transmissions are “interceptions” or “surveillance” by Google.

### **Zervas Rebuttal Opinion 2 (See Section III.B)**

5. Mr. Hochman’s assertions related to his Opinion 2 that “a major function of the tracking beacons is to collect highly personal information about users’ browsing activities [...] such as the contents of their communications with non-Google websites in the form of detailed URL requests, webpage and video interactions, and more,”<sup>8</sup> are unsupported. Mr. Hochman did not perform any analysis of how the At-Issue Data qualifies as “contents” of users’ communications with non-Google websites. Based on the definition of the term “contents” that counsel has provided me and which I have described in **Section III.B** below, I do not agree that the At-Issue Data in this case constitutes “contents” of users’ communication with non-Google websites. For example, IP address and user agent string are fields that are either required or typically included in messages that conform to the HTTP protocol. As a result, these items are more analogous to ancillary characteristics of the message that are generated in the course of communications, rather than the intended message itself. Mr. Hochman also refers to “URL requests,” “webpage and video interactions,” and “the URL of the specific webpage visited by the user,” none of which meet the definition of “contents” that counsel has provided to me, with the exception of if the URL requests also contained information such as search terms or form

---

<sup>8</sup> Hochman Report, ¶ 3.



information entered by the user (and Mr. Hochman has not identified any instances where he has found that to be the case).<sup>9</sup>

### **Zervas Rebuttal Opinion 3 (See Section III.C)**

6. Mr. Hochman’s assertions throughout his report that Google “copied” information is incorrect.<sup>10</sup> For example, Mr. Hochman argues that “Google’s tracking beacons embedded in the web page cause information to be copied from that communication and sent to Google’s servers concurrently with the user’s private communication with the non-Google website.”<sup>11</sup> My understanding of the technical definition of “copy” is the process of reading certain information from one source and writing or reproducing exactly the same information in another place. Mr. Hochman has not performed an analysis to establish that Google copied information from the communications between the user and the non-Google website.

7. Mr. Hochman incorrectly assumes that when separate communications contain the same information that means the information was “copied” from one communication to another, as opposed to being separately read from the same source. For example, Mr. Hochman refers to IP addresses as data that are copied from the user’s communication with non-Google websites. But he ignores that the IP address is assigned to the user’s device and will be the same for different communications from that device, not because the IP address value is copied from one communication to another. As a result, I do not agree with Mr. Hochman’s characterization of transmissions to Google as containing information that was “copied” from a user’s communications with non-Google websites.

---

<sup>9</sup> Hochman Report, ¶¶ 3, 96.

<sup>10</sup> See, e.g., Hochman Report, ¶¶ 45, 96, 110.

<sup>11</sup> Hochman Report, ¶ 96.

**Zervas Rebuttal Opinion 4 (See Section III.D)**

8. Mr. Hochman asserts in his Opinion 3 that “the Google tracking beacons which cause private browsing communications to be intercepted neither facilitate nor are incidental to the communications between users and non-Google websites.”<sup>12</sup> In making this assertion, Mr. Hochman fails to acknowledge that the “tracking beacons” to which he refers are integral parts of the design and operation of non-Google websites. Mr. Hochman also ignores how websites use and benefit from the Google services that use these “tracking beacons.”

9. If a website developer chooses to include Google’s (or other) services by incorporating the relevant tags into their website, those tags and the resulting services become a part of the website as it has been designed by the website developer.<sup>13</sup> Because the tags are an integral part of the website, in my opinion, the communications triggered by those tags are incidental to the communications between the user and the website. In making the claim that these communications are not incidental, Mr. Hochman implicitly assumes that a portion of the website (e.g., comprising the third-party tags) is somehow unnecessary to the website as it has been designed by the developer. I disagree with such an assumption. When a user visits a website that uses these services, she is interacting with the webpage as an entire product consisting of first- and third-party services and code as it is designed by the website developer, not as independent pieces of code that can be arbitrarily ignored.

---

<sup>12</sup> Hochman Report, ¶ 4.

<sup>13</sup> As I define in my opening report, tag is a short snippet of JavaScript code included into the HTML code of the website. These tags run as part of the website to transmit data to corresponding third-party services such as Google’s analytics and advertising services. See, Zervas Affirmative Report, ¶ 88; “HTML <script> Tag,” *W3Schools*, available at <https://perma.cc/KH7P-MY7D>.

10. When a user visits the website that includes a Google tag, her browser transmits information to Google when that tag is executed. These transmissions facilitate the communications between the user and the website because the tag itself is an integral part of the website as designed by the website developer. The transmissions also facilitate communications between the user and website because they enable the website to display the Google features (e.g., Google Ads) that the website’s developer has requested to be displayed, or enable the website developer to examine how users interact with their website (e.g., via Google Analytics) so that they can improve users’ experiences, for example. Therefore, in my opinion, these transmissions facilitate use of the website as the developer has designed it.

#### **Zervas Rebuttal Opinion 5 (See Section III.E)**

11. Mr. Hochman asserts in his Opinion 4 that “Google could have at any point before or during the class period, redesigned Chrome Incognito to either stop or limit Google’s collection of private browsing information from the private communications between users and non-Google websites.”<sup>14</sup> Mr. Hochman’s opinion is misleading and speculative, and often relies on misrepresentations of the sources he cites.

12. Mr. Hochman makes a number of speculative proposals on how Google could have redesigned its products without analyzing the feasibility of those proposals. To support his assertions, Mr. Hochman relies on selected statements of current and former Google employees that are taken out of context and therefore are misleading. I discuss examples of such statements in **Section III.E** of this report.

---

<sup>14</sup> Hochman Report, ¶ 5.

13. Mr. Hochman also presents misleading counterexamples of other browsers like Firefox and Safari, which he contends show how certain features could have functioned in Chrome. However, he ignores that these browsers generally operate in a manner similar to Chrome, and also ignores that the alternative functionality he proposes is not uniformly adopted by the different browsers that he identifies.

#### **Zervas Rebuttal Opinion 6 (See Section IV.A)**

14. Mr. Hochman's assertions related to his Opinion 5 that users are not notified about data collections when in Private Browsing Mode<sup>15</sup> and that Google could have provided such notifications<sup>16</sup> are flawed. Mr. Hochman ignores the fact that users are notified of how Private Browsing Modes function when they open a Private Browsing Session. Mr. Hochman also ignores that, consistent with Google's policies, many websites do provide notices to users about the websites' collection of data, including collection of data via Google's analytics and advertising services. I also disagree with Mr. Hochman's assertion that users were not provided a choice regarding the collection of At-Issue Data, because he ignores the variety of tools that are available to users that affect the transmissions of At-Issue Data, including tools that work even if a user is in Private Browsing Mode. For these reasons, I find Mr. Hochman's opinions regarding user notifications and user controls over the transmission of the At-Issue Data to be flawed.

---

<sup>15</sup> Hochman Report, ¶ 134.

<sup>16</sup> Hochman Report, ¶ 6.

**Zervas Rebuttal Opinion 7 (See Section IV.B)**

15. Mr. Hochman’s Opinion 6, that Google “intercepted private browsing communications without notifying websites or providing a choice at the time of collection”<sup>17</sup> is flawed. Many website developers are aware of how the technology they embed to their websites functions, and even discuss the importance of testing websites in Private Browsing Mode for various purposes. Furthermore, Mr. Hochman’s assertion that Google could provide a notification to websites at the time that Private Browsing Mode transmissions occur is based on an incorrect assumption that Google’s tags or the websites that use those tags are able to discern whether or not a user is in Private Browsing Mode. In contrast, as I discuss in **Section IV.B**, and in accord with industry recommendations, browsers are designed not to inform websites whether the user is in Private Browsing Mode. Thus, Mr. Hochman’s assertion that Google could have provided notifications to websites at the time of the Private Browsing Mode transmissions is inconsistent with industry recommendations for Private Browsing Modes.

**Zervas Rebuttal Opinion 8 (See Section V)**

16. Mr. Hochman’s Opinion 10 that “Google, throughout the class period, created detailed profiles tied to various Google identifiers (that remain undisclosed to users) based on the private browsing information it collected”<sup>18</sup> is inconsistent with the way Private Browsing Modes operate. Mr. Hochman ignores that analytics and advertising cookie values in Private Browsing Sessions are “orphaned” islands of data that are different from those sent in Regular Mode sessions and other Private Browsing Sessions. In my opening report, I demonstrated through systematic

---

<sup>17</sup> Hochman Report, ¶ 7.

<sup>18</sup> Hochman Report, ¶ 11.

testing that cookie values stored from prior Regular Mode Sessions are not used in Private Browsing Sessions and that cookie values set in a Private Browsing Session are not carried over to subsequent Regular or Private Browsing Sessions. Thus, the Private Browsing Session cookie values cannot be used to link records of user activities across different sessions or to create the “profiles” Mr. Hochman describes.

### **Zervas Rebuttal Opinion 9 (See Section VI)**

17. Mr. Hochman’s Opinion 15 alleges that Google attempted “to circumvent efforts by other companies to block Google tracking beacons.” Mr. Hochman’s arguments are overly broad and based on flawed descriptions of how certain technologies work.

18. First, Mr. Hochman asserts that “[w]ith the loss of certain Google cookies (e.g., due to blocking of certain Google cookies based on Apple’s Intelligent Tracking Prevention (‘ITP’) or Google’s [REDACTED] changes to Chrome Incognito Mode), Google mitigates targeting loss by relying on first-party identifiers, such as the PPID available for Google Ad Manager 360 Publishers.”<sup>19</sup> Mr. Hochman also asserts that “[t]his identifier is used to identify users that log into publisher websites, and it uniquely identifies a user across all of the user’s devices, browsers, and browsing sessions, including private browsing sessions.”<sup>20</sup>

19. I disagree with Mr. Hochman’s broad statements on PPID. PPID only applies when a user visits a publisher’s website which uses the PPID functionality, and the user signs in to or otherwise identifies herself to the website to allow the publisher to set the PPID. PPIDs are not the same from one publisher’s website to the next and thus cannot be used for tracking across sites.

---

<sup>19</sup> Hochman Report, ¶ 187.

<sup>20</sup> Hochman Report, ¶ 187.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

PPID values are also hashed or encrypted, rendering them meaningless to Google. And Google blocks the use of PPID for users that have opted out of personalized ads. Mr. Hochman's assertion that the use of PPID allows Google to circumvent third-party cookie blockers is incorrect for numerous reasons, including that PPID cannot be used in the same manner as third-party cookies because it is not used to track users across websites and apps operated by different publishers.<sup>21</sup> Therefore, contrary to what Mr. Hochman asserts, in my opinion, the PPID feature does not circumvent third-party cookie blockers or the tracking blocking features of the Firefox and Apple technologies Mr. Hochman identified.

20. Second, Mr. Hochman makes similar misleading statements about the feature called Enhanced Conversion. Mr. Hochman asserts that “through Enhanced Conversions in Analytics and Ads, non-Google websites send personally identifying information such as a user's email address (user's name, home address, and phone number may also be used) to Google to be matched against the same user's Google account information containing the same identifying information.”<sup>22</sup> I disagree with Mr. Hochman's statements regarding enhanced conversions, which require that a user is signed into their Google account at the time that they engage with an ad and that the user then provides some information such as an email or a phone number to the advertiser that the advertiser could send back to Google in hashed form to measure a conversion. I do not agree that the enhanced conversion feature is a replacement for third-party cookies or that its use circumvents third-party cookie blockers or the tracking blocking features of the Firefox and Apple technologies to which Mr. Hochman refers.

---

<sup>21</sup> “About publisher provided identifiers,” *Ad Manager Help*, Google, available at <https://perma.cc/P6WG-YX4S>.

<sup>22</sup> Hochman Report, ¶ 209.

**Zervas Rebuttal Opinion 10 (See Section VII)**

21. Mr. Hochman asserts in his Opinions 26 through 28 that Google “uniformly attempted to intercept all private browsing communications with non-Google websites that have a Google tracking beacon,”<sup>23</sup> that there is a “near certainty that almost every person”<sup>24</sup> that used a Private Browsing Mode had their information intercepted by Google, and that Google “does not offer users any control to escape”<sup>25</sup> its tracking beacons. I disagree with each of these assertions.

22. As described herein and in my opening report,<sup>26</sup> Google makes available to websites multiple settings that affect whether and how Google’s tags function on their website. Because those settings cause the tags’ operation to vary, I do not agree with Mr. Hochman’s assertion that Google “uniformly attempted to intercept all private browsing communications.”<sup>27</sup>

23. Contrary to Mr. Hochman’s assertion that users do not have any means to “escape” Google’s code on non-Google websites, Google and other entities have made available to users a variety of browser settings and extensions that affect whether At-Issue Data are transmitted to Google. In my opening report, I discussed and conducted tests to confirm this. Because those user settings affect the data transmissions to Google, I disagree with Mr. Hochman’s assertion that users do not have any means to “escape” Google’s code on non-Google websites, and I also disagree that users are uniformly impacted by that code.

24. Mr. Hochman also states that “[t]he Plaintiffs in this case are alleging that Google portrayed private browsing mode, including Incognito Mode, as the control to prevent Google

---

<sup>23</sup> Hochman Report, ¶ 27.

<sup>24</sup> Hochman Report, ¶ 28.

<sup>25</sup> Hochman Report, ¶ 29.

<sup>26</sup> Zervas Affirmative Report, Section V.

<sup>27</sup> Hochman Report, ¶ 27.



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

from tracking them across non-Google websites.”<sup>28</sup> I disagree with this assertion. As described in my opening report and herein, when a user enters a Private Browsing Mode in a browser, they are presented with information on how the Private Browsing Mode works and what information will still be visible to websites. As confirmed by my testing, Private Browsing Modes operate in a manner that is consistent with those descriptions. Furthermore, Private Browsing Modes like Incognito Mode do provide a measure of control and privacy for the user because any cookie values set during a Private Browsing Session are discarded at the end of the session, which is consistent with how Private Browsing Modes are described to users.

#### **Zervas Rebuttal Opinion 11 (See Section VIII)**

25. Mr. Hochman asserts in his Opinion 29 that Chrome Incognito Mode does not function the way Google states. To the contrary, in my opening report, I tested and confirmed that Incognito Mode operates as Google described to users in Incognito’s Splash Screen and “Learn More” pages, which inform users about what Incognito Mode does and does *not* do; my tests also confirmed that Private Browsing Modes in other browsers similarly operate as described to users. In particular, my tests show that Private Browsing Sessions start with a clean cookie jar, and cookie values set during such sessions are not reused in the subsequent Regular or Private Browsing Sessions. I was also able to confirm that the user’s browsing history, website logins, and autofill web forms are not carried over to the subsequent browsing sessions.

#### **Zervas Rebuttal Opinion 12 (See Section IX.A)**

26. I disagree with Mr. Hochman’s assertion in Section VIII.B of his report that “typical consumers” would not be able to understand and use browser Developer Tools.

---

<sup>28</sup> Hochman Report, ¶ 312.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Mr. Hochman does not clarify the type of consumer he has in mind or what challenges he imagines prevent them from using Developer Tools. While many users may not be inclined to use Developer Tools, some will. Developer Tools can be accessed by any user and can easily be opened, and there is an abundance of online sources that explain how to use Developer Tools. Holding a technical degree or having a deep technical background is thus not necessary to use these tools.

**Zervas Rebuttal Opinion 13 (See Section IX.B)**

27. I disagree with Mr. Hochman's assertion in Section VIII.A of his report regarding alleged negative impacts of Google's services on users' energy and device costs. In making this assertion, Mr. Hochman relies on a single article that does not even mention Google's analytics and advertising services. This assertion is also conceptually flawed, as it relies on the unreasonable assumption that if Google services disappear, no other third-party analytics and advertising services would exist and cause the same alleged impact on users' energy and device costs.

**Zervas Rebuttal Opinion 14 (See Section IX.C)**

28. Mr. Hochman asserts in Section VIII.A of his report that users do not have the option to request deletion of their Private Browsing Mode data. In my opinion, this assertion is misleading and relies on the assumption that Private Browsing Mode data are associated with a specific user, or that Google can identify Private Browsing Mode users to facilitate deletion of that data, which is inconsistent with sources upon which Mr. Hochman relies.

## II. INTRODUCTION

### A. Qualifications

29. I am an Associate Professor of Marketing at Boston University Questrom School of Business, a founding member of the Faculty of Computing & Data Sciences, and Affiliated Faculty of the Department of Computer Science. I am also a visiting researcher at Microsoft Research New England. Prior to joining the Boston University faculty, I held academic roles including visiting scholar at the MIT Sloan School of Management, Simons Postdoctoral Fellow at Yale University, and affiliate at the Center for Research on Computation and Society at Harvard University's John A. Paulson School of Engineering and Applied Sciences. I am an associate editor of ACM Transactions on Economics and Computation, and I sit on the editorial review boards of Marketing Science, the Journal of Marketing Research, and the Journal of Marketing.

30. My research, which falls in the broader area of digitization, combines methods from computer science and economics to study online marketplaces to understand their impact on consumer and firm behavior. I have conducted studies on online marketplaces such as Airbnb, Yelp, TripAdvisor, and Expedia. My work is empirical in nature and relies on assembling and analyzing novel sources of data that I collect from these marketplaces to study their operation. I hold a Bachelor of Engineering and a Master of Science in Computer Science from Imperial College in London, a Master of Arts in Interactive Media from London College of Communication, and a Ph.D. in Computer Science from Boston University. Before pursuing my Ph.D. in computer science, I ran a small information technology (IT) company. My C.V. is attached as **Appendix A**, and a list of my prior testimony is attached as **Appendix B**.

31. I am being compensated at the rate of \$700 per hour for my time on this case. Research and analysis for this report was also performed by Analysis Group personnel under my

direction and guidance. My compensation is not contingent upon my findings, the testimony I may give, or the outcome of this litigation.

32. On April 15, 2022, I submitted an opening report and offered opinions on the relevant technology at issue: Private Browsing Modes in Chrome and other browsers and Google’s advertising or analytics services<sup>29</sup> offered to third-party websites.

**B. Assignment**

33. I have been engaged in this matter by counsel for Google LLC (“Google”) to respond to certain opinions in the Expert Report of Jonathan E. Hochman (“Hochman Report”).

34. Mr. Hochman was retained by counsel for the Plaintiffs “to develop and render opinions concerning the technology and practices at issue in this litigation with respect to several products.”<sup>30</sup> The products included in Mr. Hochman’s report include “those utilizing Google tracking code (e.g., Google Analytics and conversion tracking code) and Google advertising code (e.g., Google Ad Manager and Google AdSense advertising code).”<sup>31</sup>

35. In this report, I have been asked to review and respond to certain opinions presented in Mr. Hochman’s report regarding Google’s analytics and advertising services and Private Browsing Modes. My opinions are described in this report.

36. My failure to address any specific sentence or opinion in Mr. Hochman’s report does not mean that I agree with it, and no such agreement should be inferred.

---

<sup>29</sup> Throughout this report, I refer to specific Google services by their names (e.g., Google Analytics, Google Ad Manager, Google Analytics 360). I refer to Google’s analytics services and Google’s advertising services as a collection of respective tools.

<sup>30</sup> Hochman Report, ¶ 54.

<sup>31</sup> Hochman Report, ¶ 54.

**C. Facts And Data Considered**

37. In forming my opinions, I have relied upon my professional and academic experience and reviewed documents obtained from public sources. I also relied on the data and analysis based on the experiments I conducted in my opening report. I have also reviewed and relied upon the deposition testimony of Google witnesses and documents produced by Google in this case.

38. The sources I considered in forming my opinions are identified in this report and the accompanying exhibits and are listed in the attached **Appendix C**.

39. Should additional relevant documents or information be made available to me, I reserve the right to supplement my opinions as appropriate.

**III. REBUTTAL TO MR. HOCHMAN’S DESCRIPTIONS OF GOOGLE’S ANALYTICS AND ADVERTISING SERVICES****A. Mr. Hochman’s Assertions That Google “Intentionally Intercepts” Private Browsing Communications Are Inaccurate (Hochman Opinion 1)**

40. In his Opinion 1, Mr. Hochman contends that “Google, by way of various tracking beacons, intercepted private browsing communications between users and non-Google websites while those communications were in transit.”<sup>32</sup> Mr. Hochman similarly offers an opinion that “Google, throughout the class period, intentionally intercepted private browsing communications between users and non-Google websites while those communications were in transit and collected private browsing information from those communications.”<sup>33</sup> As support for these statements, Mr. Hochman describes the functionality of what he calls Google’s “tracking code” or “tracking

---

<sup>32</sup> Hochman Report, ¶ 2.

<sup>33</sup> Hochman Report, ¶ 78.

and advertising code.”<sup>34</sup> In my opinion, Mr. Hochman’s descriptions of that code and how it functions are both inaccurate and misleading.

41. As an initial matter, throughout his report, Mr. Hochman uses phrases like “tracking and advertising products,” “tracking and advertising code,” and “tracking beacons” to describe multiple different products, including Classic Google Analytics, Google Analytics 360, Google Analytics 4, Universal Analytics, Google Ad Manager, and Google AdSense.<sup>35</sup> However, as described in my opening report, these are distinct products.<sup>36</sup> Mr. Hochman uses these phrases in his report to make broad statements, and at times incorrectly implies that his description of the features or functionality of one product is common to the entire group of products. For example, Mr. Hochman asserts that “Google tracking beacons throughout the class period had a common functionality in terms of Google’s interception and data collection, not limited to the Analytics and Ad Manager codes.”<sup>37</sup> Because Analytics and Ad Manager are distinct products with different features, I disagree with Mr. Hochman to the extent he asserts that they have a “common functionality.”

42. In his report, Mr. Hochman repeatedly characterizes communications sent to Google as “interceptions.” For example, Mr. Hochman asserts:

---

<sup>34</sup> Hochman Report, ¶¶ 79-80.

<sup>35</sup> Hochman Report, ¶¶ 79-80, fn. 6, 8.

<sup>36</sup> See e.g., Zervas Affirmative Report, Section V.

<sup>37</sup> Hochman Report, ¶ 84.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

- “Google Interception: Throughout the class period, Google intentionally intercepted private browsing communications between users and non-Google websites while those communications were in transit.”<sup>38</sup>
- “It is my opinion that Google, throughout the class period, intentionally intercepted private browsing communications between users and non-Google websites while those communications were in transit and collected private browsing information from those communications.”<sup>39</sup>
- “Google Analytics tracking beacons intercept private communication between the user and the non-Google website’s server and send the intercepted communication to Google.”<sup>40</sup>
- “Google intercepts private browsing information through tracking beacons designed by Google to intercept and collect information from communications between users and non-Google websites, including while users are in a private browsing mode.”<sup>41</sup>
- “The fundamental operation of the Google tracking beacon for the purpose of intercepting private browsing information at issue in the case is independent of the device and browser.”<sup>42</sup>

---

<sup>38</sup> Hochman Report, Section VIII.A. Description.

<sup>39</sup> Hochman Report, ¶ 78.

<sup>40</sup> Hochman Report, Appendix A, ¶ 17.

<sup>41</sup> Hochman Report, ¶ 83.

<sup>42</sup> Hochman Report, Appendix B, ¶ 13.

43. Mr. Hochman also uses the phrase “surveillance of the user” in describing the Google Analytics product.<sup>43</sup> In my opinion, persons who are familiar with how modern websites operate and how browsers communicate with those websites, even at a general level, would not use terms like “interception” or “surveillance” to describe Google’s receipt of information related to a user’s visit to a website that uses Google’s analytics or advertising services; nor would such a characterization be consistent with the mechanics of how these communications take place. Thus, Mr. Hochman’s use of terms such as “intercepted,” “intentionally intercepted,” and “surveillance” to describe Google’s analytics and advertising services is incorrect and misleading.

44. Mr. Hochman ignores that these communications to Google only happen because websites have chosen to utilize one or more of Google’s analytics or advertising services. Google offers these services to website developers, but the developers make the decision themselves to use the services and incorporate the associated Google tags or any other code. For example, as I described in Sections V.A and V.B of my opening report, to use Google Analytics and Google Ad Manager services, website developers must incorporate “tags, which are short snippets of JavaScript code, into the HTML source code for their website.”<sup>44</sup> If the website developers do not incorporate the Google tags necessary to enable the Google service, the communications to Google that Mr. Hochman describes would not occur.

45. To illustrate this point, I visited <https://www.wikipedia.org/>, a website that does not incorporate Google tags, using the Chrome browser in Incognito Mode and recorded the browser’s communications using Chrome Developer Tools. As shown in **Figure 1** below, I observed eight

---

<sup>43</sup> Hochman Report, Appendix A, ¶ 17.

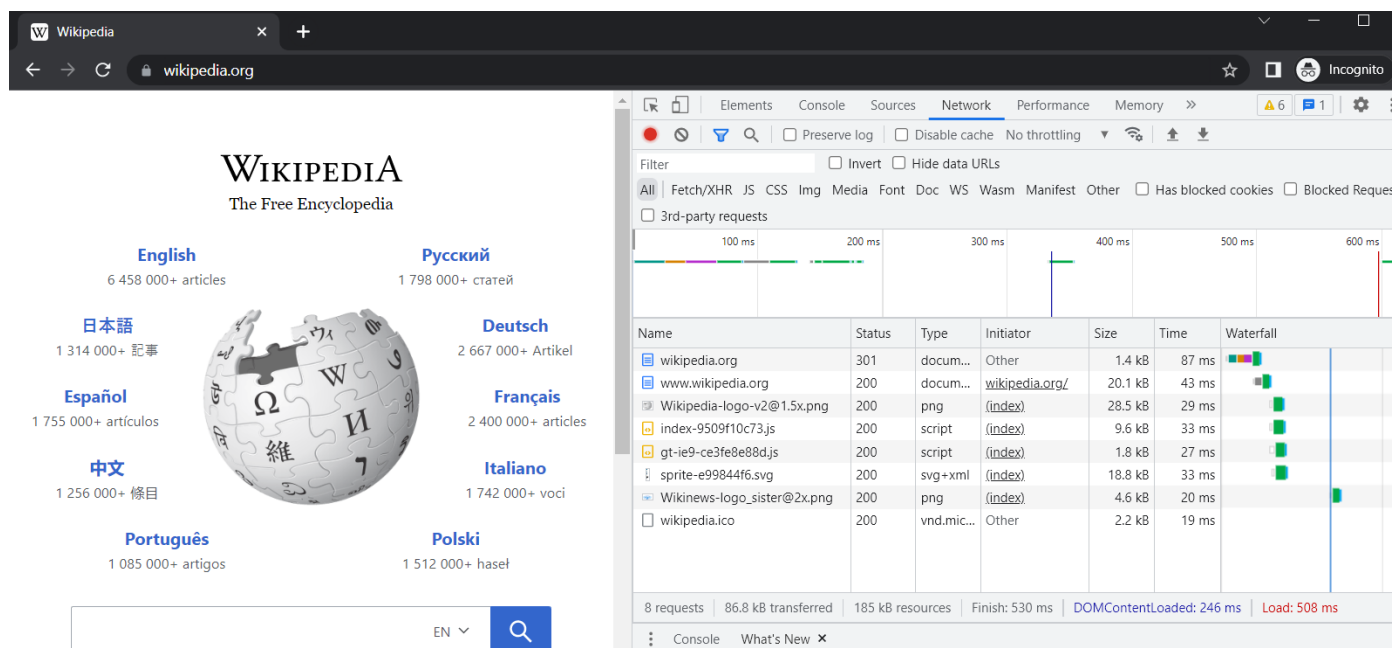
<sup>44</sup> Zervas Affirmative Report, ¶ 88.



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

separate HTTP requests, none of which were to the domains associated with Google.<sup>45</sup> This is consistent with my expectations, because *wikipedia.org* does not incorporate the tags that would trigger transmissions to Google. In characterizing Google’s receipt of information as an “interception,” Mr. Hochman ignores the fact that those transmissions are a result of the website developer’s installation of the relevant Google tags on their website.

**Figure 1**  
**Wikipedia.org Home Page Without Communications to Google**



46. Mr. Hochman also ignores that the relevant Google tags can be configured by website developers who choose to use Google’s analytics or advertising services, and there are settings available to those developers that would affect the transmission of At-Issue Data to Google via those tags. In Sections V.A.1 and V.B.1 of my opening report, I described several ways website developers and publishers can affect transmissions of At-Issue Data to Google. For example,

<sup>45</sup> I describe HTTP requests in Section III.B of my opening report.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Google Analytics provides website developers a way to disable Google Analytics functionality on a webpage to honor visitors’ opt-out choices, without removing the Google Analytics tag itself.<sup>46,47</sup> When this feature is enabled, it will prevent the Google Analytics tag from storing cookie values and sending them to Google Analytics.”<sup>48,49</sup> Google Analytics also provides an Analytics User ID feature, but these User IDs are generated, assigned, and managed by the first-party website.<sup>50</sup> If a website developer does not enable or configure this feature, User ID data will not be sent to Google Analytics. Similarly, Google Ad Manager provides a setting “to serve ‘limited ads,’” which are ads that “disable all personalization and features that require use of a local identifier.”<sup>51,52</sup>

47. As discussed in my opening report, modern websites typically use multiple third-party services similar to those Google provides.<sup>53</sup> Google offers website developers a significant amount of information regarding how the tags that enable its services work, and it is my expectation that developers use the tags with full knowledge that they are designed to automatically send information to Google when users visit their websites (subject to various settings available to the website developer and to browser users).

---

<sup>46</sup> “Disable Google Analytics measurement,” *Google Analytics, Google*, available at <https://perma.cc/FXP9-3CGT>.

<sup>47</sup> “Manage user privacy,” *Google Analytics, Google*, available at <https://perma.cc/PVW7-EBB2>.

<sup>48</sup> “Disable Google Analytics measurement,” *Google Analytics, Google*, available at <https://perma.cc/FXP9-3CGT>.

<sup>49</sup> “Manage user privacy,” *Google Analytics, Google*, available at <https://perma.cc/PVW7-EBB2>.

<sup>50</sup> “User-ID limits,” *Analytics Help, Google*, available at <https://perma.cc/V6BT-9A8X>.

<sup>51</sup> Zervas Affirmative Report, ¶ 95; “Disable Google Analytics measurement,” *Google Analytics, Google*, available at <https://perma.cc/FXP9-3CGT>; “Manage user privacy,” *Google Analytics, Google*, available at <https://perma.cc/PVW7-EBB2>; Zervas Affirmative Report, ¶ 110; “Limited Ads,” *Google Ad Manager Help, Google*, available at <https://perma.cc/MT25-D2C3>.

<sup>52</sup> I discuss other options available to websites and users in more detail in **Sections VII** and **IX** of this report.

<sup>53</sup> Zervas Affirmative Report, ¶ 39.

48. I am also aware that some website developers perform testing of their websites in Private Browsing Mode, for example to test how the website will work when users visit the site in a Private Browsing Mode.<sup>54</sup> It is also well known in the industry that Private Browsing Modes are designed not to inform websites of users' private browsing status. For example, the W3C states that "when the differences in browser behavior between privacy and standard browsing modes can be detected because of standardization or implementation details, websites might choose to degrade browsing experience (for example, not displaying content) when they detect the users in private browsing modes. This is undesirable."<sup>55</sup> The W3C further states, "browser vendors should work towards achieving private browsing mode work in a way indistinguishable for [...] sites from the normal mode, to respect the user's [...] privacy [...]."<sup>56</sup>

49. Based on the public information identified above, I expect that website developers are aware of how the tags for Google's advertising and analytics operate and how Private Browsing Modes work, including the fact that browsers do not identify whether a user is in Regular or Private Browsing Mode. Mr. Hochman has not identified, and I have not seen, any evidence indicating that website developers are not aware that third-party services such as Google's analytics and advertising services operate in Private Browsing Modes similarly to how they operate in Regular Browsing Modes. It is thus incorrect to claim that Google "intercepted," "intentionally intercepted," and conducted "surveillance" through its analytics and advertising services.

---

<sup>54</sup> "Strategies for carrying out testing," *MDN Web Docs*, available at <https://perma.cc/F5G6-KN2C>.

<sup>55</sup> "W3C TAG Observations on Private Browsing Modes," *W3C*, July 5, 2019, available at <https://perma.cc/5CHW-LNER>.

<sup>56</sup> "W3C TAG Observations on Private Browsing Modes," *W3C*, July 5, 2019, available at <https://perma.cc/5CHW-LNER>.

**B. Mr. Hochman Does Not Provide Any Support For His Opinion That “Tracking Beacons” Collect The Content Of Users’ Communications (Hochman Opinion 2)**

50. In his Opinion 2, Mr. Hochman states that “a major function of the ‘tracking beacons’ is to collect highly personal information about users’ browsing activities [...] such as the contents of their communications with non-Google websites in the form of detailed URL requests, webpage and video interactions, and more.”<sup>57</sup>

51. I understand Google disputes that the At-Issue Data<sup>58</sup> constitute “contents” under applicable laws. While I do not offer an opinion on the meaning of the term “contents” in this context, I understand from counsel that for purposes of Plaintiffs’ claims in this case, “contents” refers to the intended message conveyed by the communication and does not include information generated in the course of the communication that is used to facilitate delivery of the message. I have also been asked by counsel to assume that (1) URLs of pages visited alone are not “content”; and (2) to qualify as “content,” URLs must contain the user’s search terms, not just the webpage the user was viewing. For example, while an HTTP request could theoretically include search terms or messages from a user, these are not required fields and whether a particular HTTP request in fact contains “contents” requires analysis of the information contained in the message.

52. Mr. Hochman did not analyze what specific information constitutes “contents of [users’] communications with non-Google websites.”<sup>59</sup> Instead, he generally refers to “detailed URL requests, webpage and video interactions, and more,” and subsequently asserts that information Google collected includes “the URL of the specific webpage visited by the user

---

<sup>57</sup> Hochman Report, ¶ 3.

<sup>58</sup> Zervas Affirmative Report, ¶ 14.

<sup>59</sup> Hochman Report, ¶ 3.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

(including the full URL viewed by the user on the non-Google website, which would include folders, subfolders, and precise file requested from the webserver), the user’s IP address, and the user agent string of the user’s browser, among other information.”<sup>60</sup> Based on the definition described above, I do not agree that this information constitutes “contents” of a user’s communication with the non-Google website. The IP address and user agent string are fields that are either required or typically included in messages that conform to the HTTP protocol, and thus are information used to facilitate delivery of the message that are generated in the course of communications, not the intended message itself. As a result, these items are more analogous to ancillary characteristics of the message that are generated in the course of communications, rather than the intended message itself. Mr. Hochman also refers to “URL requests,” “webpage and video interactions,” and “the URL of the specific webpage visited by the user,” each of which is similar to URLs of pages visited, which is not “contents” under the definition of that term counsel has provided to me, with the exception of if the URL requests also contained information such as search terms or form information entered by the user (and Mr. Hochman has not identified any instances where he has found that to be the case).

**C. Mr. Hochman Fails To Establish That Google “Copied” Information From Users’ Communications**

53. In multiple assertions throughout his report, Mr. Hochman uses the term “cop[y]” to describe Google’s services in a way that is misleading and unsupported.<sup>61</sup> For example, Mr. Hochman makes the following assertions:

---

<sup>60</sup> Hochman Report, ¶¶ 3, 96.

<sup>61</sup> Hochman Report, ¶ 96.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

- “Google tracking beacons use the Chrome browser to copy and send users’ browsing history to Google servers.”<sup>62</sup>
- “Google’s tracking beacons embedded in the web page cause information to be copied from that communication and sent to Google’s servers concurrently with the user’s private communication with the non-Google website.”<sup>63</sup>
- “Google tracking beacons are loaded and used by Google to intercept communications between users and non-Google websites to obtain information that is contemporaneously copied from the initial GET message and sent to Google servers.”<sup>64</sup>

54. Mr. Hochman does not provide a definition of what he means by “copy” in this context. For example, one definition of “copying” in computer science is a process that “creates an exact image of a file on a disk with different file name.”<sup>65</sup> In other words, the term “copy” is the process of reading certain information from one source and writing or reproducing exactly the same information in another place. Mr. Hochman has not shown any evidence that the information he asserts as “copied” originated from users’ communication with non-Google websites.

55. For example, Mr. Hochman asserts that the information “copied” from users’ communications with non-Google websites includes “user’s IP address, and the user agent string of the user’s browser among other information.”<sup>66</sup> Mr. Hochman has not identified any evidence supporting his assertion that IP address and user agent strings are “copied” from these

---

<sup>62</sup> Hochman Report, ¶ 45.

<sup>63</sup> Hochman Report, ¶ 96.

<sup>64</sup> Hochman Report, ¶ 110.

<sup>65</sup> “cp command in Linux with examples,” *GeeksforGeeks*, February 19, 2021, available at <https://perma.cc/2TV6-H3DY>.

<sup>66</sup> Hochman Report, ¶ 96.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

communications. As I discuss in my opening report, an IP address is an essential component of internet communications because it informs a client and a server where the information should be sent.<sup>67</sup> Similarly, the “User-Agent” field is present in most HTTP requests and is used to inform the server about the user’s device and web browser. This information can be used to display content to a user.<sup>68</sup> As long as a user’s IP address does not change (as happens, for example, if the user connects to another network), and as long as a user agent does not change (as happens, for example, if a user decides to browse with another device or browser), these types of information will be identical across different requests, even if users visit different websites. But the fact that the IP address and user agent are the same does not mean they are “copied” from the communications with the website’s servers, as Mr. Hochman asserts. To the contrary, this is information transmitted in HTTP requests as a basic aspect of Internet communications. Mr. Hochman incorrectly assumes that when separate communications contain the same information that means the information was “copied” from one communication to another, as opposed to being separately read from the same source.

56. Because of the above, and because Mr. Hochman has not identified any evidence that information sent to Google is “copied” from the communications between a user and third-party website rather than as part of regular internet communications, I disagree with his assessment of how Google’s analytics and advertising services operate.

---

<sup>67</sup> See e.g., Zervas Affirmative Report, ¶ 24.

<sup>68</sup> “Definition of User Agent,” *W3C*, June 16, 2011, available at <https://perma.cc/5FCX-K45N>; “HTTP headers | User-Agent,” *GeeksforGeeks*, October 11, 2019, available at <https://perma.cc/QAA8-S428>.

**D. Mr. Hochman’s Assertion That Google “Tracking Beacons” “Neither Facilitate Nor Are Incidental To” Users’ Communications With Websites Is Incorrect (Hochman Opinion 3)**

57. In his Opinion 3, Mr. Hochman asserts that “the Google tracking beacons which cause private browsing communications to be intercepted neither facilitate nor are incidental to the communications between users and non-Google websites.”<sup>69</sup> In offering this opinion, Mr. Hochman ignores how websites use and benefit from Google’s services. This statement is also incorrect because it fails to take into account how web browsing technologies generally operate and why third-party services exist.

58. Modern websites are a combination of first- and third-party code. While websites appear as unified pages to the user, they typically draw on many different files from various sources. As I explained in my opening report, third-party services allow for efficient software development by leveraging code reusability, which allows separate entities to develop and maintain a smaller part of code.<sup>70</sup> As I further discussed in my opening report, certain functionalities enabled by JavaScript code are complex and inefficient, if not impossible, for most websites to develop or replicate on their own.<sup>71</sup> As a result, many smaller-scale businesses would find it prohibitive to develop and maintain features that are provided by third-parties, such as Google. Availability of such services enables businesses to compete for online presence and improve business performance.<sup>72</sup>

---

<sup>69</sup> Hochman Report, ¶ 4.

<sup>70</sup> Zervas Affirmative Report, ¶ 39.

<sup>71</sup> Zervas Affirmative Report, ¶ 39.

<sup>72</sup> “Three Ways APIs Are Keeping Small Businesses Digitally Competitive,” *Small Business Trends*, February 10, 2022, available at <https://perma.cc/6W7V-ZR5N>; Berman, Ron, and Ayelet Israeli, “The Value of Descriptive Analytics: Evidence from Online Retailers,” *Harvard Business School*, Working Paper 21-067, 2021, available at <https://perma.cc/B7JY-V3UX>; Benzell, Seth G., Guillermo Lagarda,



59. Mr. Hochman provides a misleading and one-sided opinion discussing only the alleged negative impacts of Google’s analytics and advertising services, while ignoring the fact that those services are necessary for websites. For example, advertising is an important source of revenue without which many websites would not exist and/or would not be able to provide free content to users without charging subscription fees.<sup>73</sup>

*I. Google’s Analytics And Advertising Services And Related Tags Facilitate And Are Incidental To Users’ Communications With Websites*

60. I disagree with Mr. Hochman’s assertion that Google’s analytics and advertising services “neither facilitate nor are incidental to the communications between users and non-Google websites.”<sup>74</sup> In my opinion, Google’s analytics and advertising services do facilitate and are incidental to communications between users and websites that use Google services because the websites have chosen to make Google services *part of the website*.

61. It is common for modern websites to include third-party services that are required to enable certain functionality such as styling, payment methods, maps, analytics, videos, or advertising. Websites often use multiple Google and non-Google third-party services. For example, I visited Plaintiffs’ attorneys’ website <https://www.forthethepeople.com/> in Incognito Mode and recorded all transmissions on the home page using Chrome Developer Tools. Just visiting the home page triggered transmissions to 61 third-party domains, only a portion of which were

---

and Marshall Van Alstyne, “The Impact of APIs on Firm Performance,” *Boston University Questrom School of Business Research Paper*, available at <https://perma.cc/5FRY-WTSF>.

<sup>73</sup> “Ad-Supported vs Subscription: Which is Better,” *Aniview*, December 11, 2021, available at <https://perma.cc/7NN2-XFEY>.

<sup>74</sup> Hochman Report, ¶ 4.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

associated with Google. **Figure 2** illustrates the top ten third-party domains that I observed in terms of the number of transmissions associated with each respective domain.<sup>75</sup>

**Figure 2**  
**Transmissions To Third-Party Domains When Loading <https://www.forthethepeople.com/>**

Domain	Number of Transmissions
<i>wistia.com</i>	116
<i>litix.io</i>	29
<i>simpli.fi</i>	23
<i>tiktok.com</i>	14
<i>doubleclick.net</i>	12
<i>clarity.ms</i>	10
<i>mouseflow.com</i>	9
<i>cookielaw.org</i>	8
<i>gstatic.com</i>	8
<i>tctm.co</i>	7

62. If a website developer chooses to include Google (or other) services by incorporating the relevant tags into their website, those tags and the resulting services become part of the website as it has been designed by the website developer. Because the tags are an integral part of the website, in my opinion the communications triggered by those tags are incidental to the communications between the user and the website. In making the claim that these communications are not incidental, Mr. Hochman implicitly assumes that a portion of the website (e.g., comprising

---

<sup>75</sup> I listed all domains and the corresponding number of observed transmissions in my backup materials.

the third-party tags) is somehow unnecessary to the website as it has been designed by the developer. I disagree with such an assumption. When a user visits a website that uses these services, she is interacting with the webpage as an entire product consisting of first- and third-party services and code as it is designed by the website developer and not as independent pieces of code that can be arbitrarily ignored.

63. When a user visits the website that includes a Google tag, her browser transmits information to Google when that tag is executed so that Google can provide the service requested. These transmissions facilitate the user's communications with the website because the third-party services that the website's developer has chosen to install on their site are *part of the website*. The transmissions also facilitate communications between the user and the website since they enable the website to display Google features (e.g., Google Ads) that the website's developer has requested to be displayed and/or enable the website's developer to examine how users interact with said website (e.g., Google Analytics).

## 2. *Importance Of Analytics Services*

64. Mr. Hochman fails to acknowledge the benefits of Google's analytics services, which allow websites to understand who their users are and how they interact with the website, which is important for developing user-friendly designs.<sup>76</sup> Using these insights, websites can constantly modify their product and understand which features users value. As a result, website developers may consider focusing on developing certain functionalities or adding certain features

---

<sup>76</sup> See, Garrett, Renee et al., "A Literature Review: Website Design and User Engagement," *Online journal of communication and media technologies*, Vol. 6, No. 3, 2016, pp. 1-14, available at <https://perma.cc/PPC7-PWCM>; Sabanovic, Edin, "How to Use Google Analytics to Improve Your Web Design Projects," *Shopify Partners, Shopify*, June 13, 2017, available at <https://perma.cc/QG8Y-JYD8>.

that might be of interest to users. For example, website developers might notice a substantial flow of users from certain geographical regions and adopt a version of the website in another language. Similarly, using insights from web analytics on the most common interactions of users with their desktop websites and information on the characteristics of users' devices, site owners can adapt their websites to user-friendly mobile versions.<sup>77</sup> The absence of analytics services would prevent websites from receiving important insights on their user base, which would hinder the implementation of user-centric web development.

65. In his report, Mr. Hochman attempts to negate the importance of analytics and advertising services by saying that “a major function of the tracking beacons is to collect highly personal information about users’ browsing activities.”<sup>78</sup> However, that does not comport with Mr. Hochman’s statements outside of this litigation. For example, I reviewed Mr. Hochman’s website <https://www.hochmanconsultants.com/>, which I understand is the website of a firm Mr. Hochman founded “to help businesses of all sizes better leverage the opportunities that the Internet provides.”<sup>79</sup> On his website, Mr. Hochman encourages websites to “[u]se web analytics to learn from your visitors.”<sup>80</sup> For example:

- “[e]very business needs to know: How many visitors come to the site? What are the sources of visitor referrals? What keywords do visitors use? What pages attract the most interest? How many visitors are completing the objective?”<sup>81</sup>

---

<sup>77</sup> Tidal, Junior R., “Using Web Analytics for Mobile Interface Development,” *New York City College of Technology*, 2013, available at <https://perma.cc/Z6Z8-U5MW>.

<sup>78</sup> Hochman Report, ¶ 3.

<sup>79</sup> “About Us: Helping your business leverage the Internet,” *Hochman Consultants*, available at <https://perma.cc/86E7-A39K>.

<sup>80</sup> “The Internet Marketing Process,” *Hochman Consultants*, available at <https://perma.cc/Y354-MANZ>.

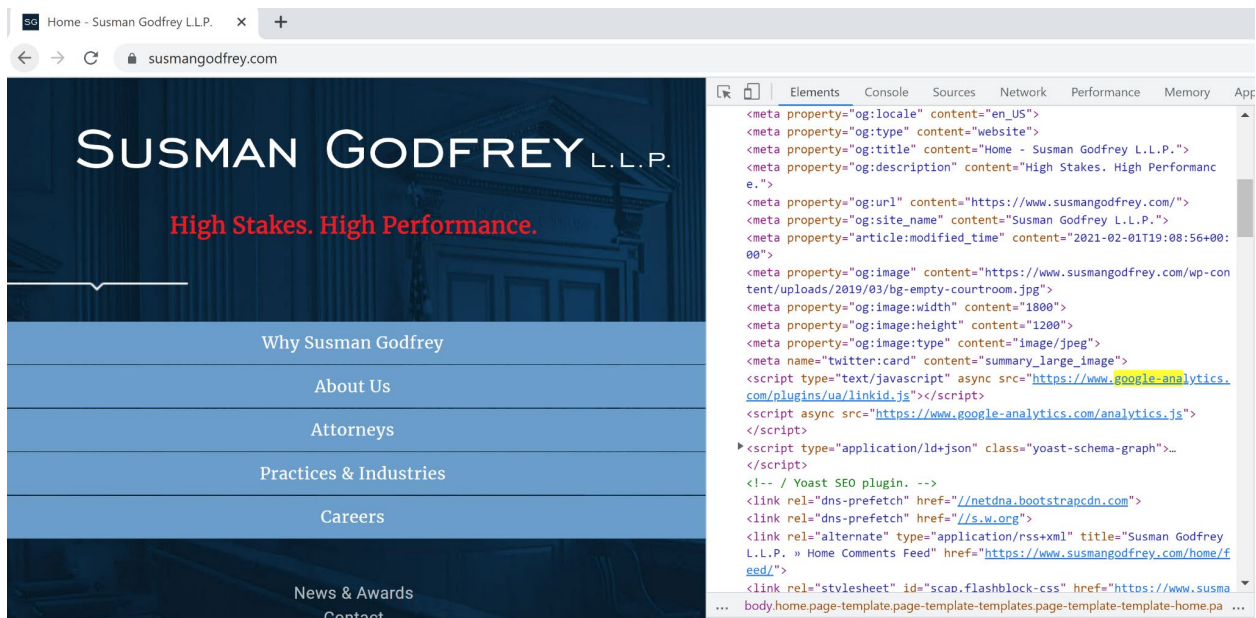
<sup>81</sup> “The Internet Marketing Process,” *Hochman Consultants*, available at <https://perma.cc/Y354-MANZ>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

- “[t]hat’s just the beginning of what you can learn with web analytics. Depending upon the specific nature of your business, may need to know: the geographic distribution of your visitors, how many customers you lose at each step in your checkout process, or the pages that cause visitors to leave your site.”<sup>82</sup>

66. Similarly, the websites for all three Plaintiffs’ attorneys Susman Godfrey L.L.P (<https://www.susmangodfrey.com>), Boies Schiller Flexner LLP (<https://www.bsflp.com>), and Morgan & Morgan Lawyers (<https://www.forthethepeople.com>) use a variety of Google services. For example, **Figures 3** through **5** below illustrate the inclusion of Google Tags in websites of all three Plaintiffs’ attorneys:

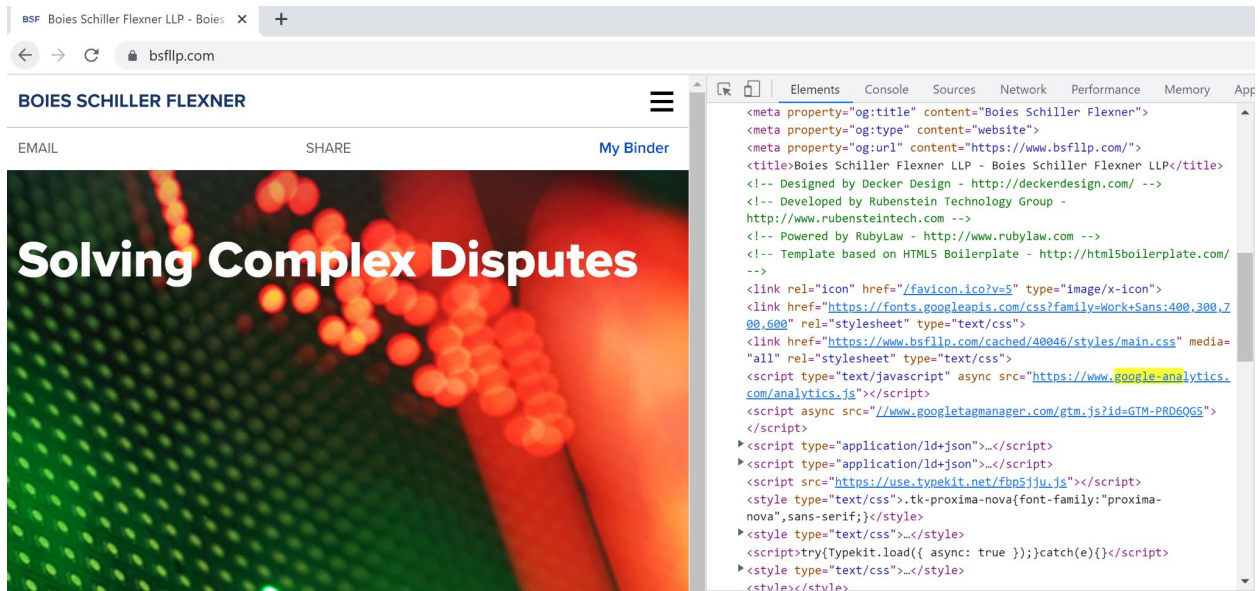
**Figure 3**  
**Example Of Google Analytics Tag In Susman Godfrey L.L.P Website**



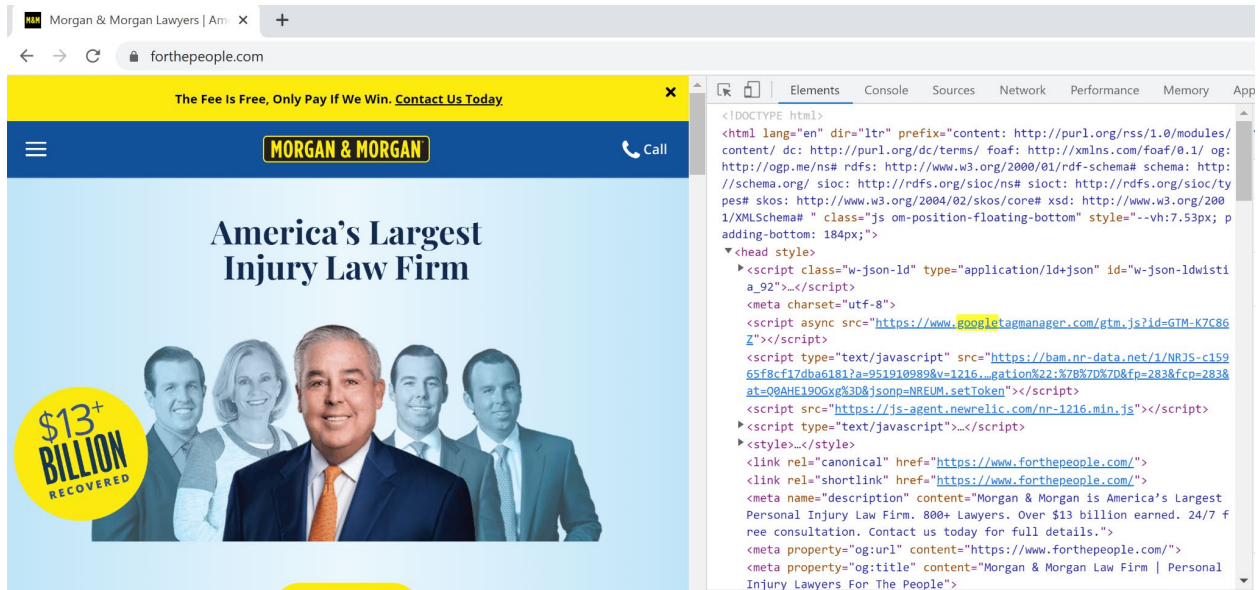
<sup>82</sup> “The Internet Marketing Process,” *Hochman Consultants*, available at <https://perma.cc/Y354-MANZ>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure 4**  
**Example Of Google Analytics Tag In Boies Schiller Flexner LLP Website**



**Figure 5**  
**Example Of Google Tag In Morgan & Morgan Lawyers Website**



67. The inclusion of Google Analytics in the websites for *all three* of Plaintiffs' law firms—years after they filed this case—illustrates the importance of these services. Since the



inclusion of these tags in a website's source code is a voluntary decision websites make, these services will only be included if the website developers find these services valuable.

### 3. *Importance Of Advertising To Websites And Users*

68. Digital advertising services are important to optimize efficiency of advertising campaigns, which are an important source of website financing.<sup>83</sup> Advertising revenues allow websites to operate and provide content to users without subscription fees.<sup>84,85</sup> For example, websites' users can access a wide range of free ad-sponsored content that would otherwise be unavailable to them. Such services range from news media—with free websites such as Vox, CNN, and Fox News hosting ads on their sites—to video entertainment—with websites such as Crackle and Peacock offering free ad-supported entertainment.

69. Because advertising provides another revenue stream for website owners and operators, ads expand the size of the online ecosystem, making more resources available to users.<sup>86</sup> One study found that the ad supported internet ecosystem doubled its contribution to the US economy between 2012 and 2016.<sup>87</sup> Online advertising also reduces the cost individual users have

---

<sup>83</sup> For instance, in 2020, US newspaper companies generated 39 percent of their advertising revenue from digital advertising. See, “Share of digital in newspaper advertising revenue in the United States from 2011 to 2020,” *Statista*, available at <https://perma.cc/P88K-7CQK>.

<sup>84</sup> Klym, Natalie and David Clark, “The Future of the Ad-Supported Internet Ecosystem,” *MIT Internet Policy Research Initiative*, 2019, p. 2, available at <https://perma.cc/S6LC-KHPJ>.

<sup>85</sup> For instance, Peacock, a popular video-streaming service, offers a free ad-supported subscription, alongside paid-for ad-free options. See, “Choose a Plan,” *Peacock*, available at <https://perma.cc/MLK5-GX59>.

<sup>86</sup> Deighton, John, A., and Leora D. Kornfeld, “Economic Value of the Advertising-Supported Internet Ecosystem,” *Interactive Advertising Bureau*, September 2012, available at <https://perma.cc/2SS5-CGJK>.

<sup>87</sup> “Ad-Supported Internet Brings over \$1 Trillion to the U.S. Economy, Representing 6 Percent of Country's Total GDP, According to IAB Study Led by Harvard Business School Professor,” *Interactive Advertising Bureau*, March 15, 2017, available at <https://perma.cc/G9BS-85MJ>.

to pay in order to benefit from online content.<sup>88</sup> In addition, advertising is one of the main ways for commercial digital media to generate a profit.<sup>89</sup>

70. In his report, Mr. Hochman presents an example of *The New York Times* website being opened in Firefox Private Browsing Mode without ads.<sup>90</sup> Mr. Hochman fails to acknowledge that his visit to *The New York Times* using Firefox in Private Browsing Mode that did not contain observed ads was possible because many other users *do* observe ads when visiting *The New York Times*. The users who are displayed ads subsidize his ads-free visit. In the absence of ads, users likely would have to pay either higher subscription fees or would not even have access to *The New York Times* online as ads are an important source of revenues required for many websites to keep operating.<sup>91</sup> The academic literature acknowledges the benefits produced by digital ad-supported content, going as far as to discuss whether these benefits should be captured in GDP measures.<sup>92</sup> One estimate, which models consumer surplus by considering leisure time spent on the internet, suggests that free internet services might create over \$100 billion in consumer surplus per year in

---

<sup>88</sup> Deighton, John, A., and Leora D. Kornfeld, “Economic Value of the Advertising-Supported Internet Ecosystem,” *Interactive Advertising Bureau*, September 2012, available at <https://perma.cc/2SS5-CGJK>.

<sup>89</sup> Bekh, Alona, “Advertising-based Revenue Model in Digital Media Market,” *Ekonomski vjesnik/Econviews - Review of Contemporary Business, Entrepreneurship and Economic Issues*, Vol. 33, No. 2, 2020, p. 548, available at <https://perma.cc/W7QP-YTPM>.

<sup>90</sup> Hochman Report, ¶ 115.

<sup>91</sup> For example, the New York Times derived over \$116M in revenue in the first quarter of 2022 from advertising. See, “The New York Times Company Reports First-Quarter 2022 Results,” *The New York Times Company*, May 4, 2022, available at <https://perma.cc/QR4R-EHP6>.

<sup>92</sup> See, Nakamura, Leonard, Jon Samuels, and Rachel Soloveichik “Valuing ‘Free’ Media in GDP: An Experiment Approach,” *Federal Reserve Board of Philadelphia Working Paper*, No. 16-24, 2016, available at <https://perma.cc/4HMJ-7D3R>; Ahmad, Nadim, and Paul Schreyer, “Measuring GDP in a Digitalized Economy,” *OECD Statistics Working Papers*, No. 2016/07, 2016, available at <https://perma.cc/GNV6-GHRX>.



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

the U.S., corresponding to about 0.74 percent of annual GDP.<sup>93</sup> Another estimate found that welfare gains associated with the expansion of free media goods arising from the advent of digital advertising led to a 2.5 and 2.7 percent increase in welfare in terms of consumption for the non-college- and college-educated population specifically.<sup>94</sup>

71. Mr. Hochman also writes in Appendix A to his report that “[he has] used Google AdWords (now known as Google Ads) since 2003 for hundreds of different clients and thousands of different campaigns.”<sup>95</sup> Thus, outside of this litigation, it appears that Mr. Hochman understands and supports the value of Google’s advertising services.

**E. Mr. Hochman’s Assertion That Google Could Have Designed Chrome Differently Is Speculative And Misleading (Hochman Opinion 4)**

72. In his Opinion 4, Mr. Hochman asserts that “Google could have at any point before or during the class period, redesigned Chrome Incognito to either stop or limit Google’s collection of private browsing information from the private communications between users and non-Google websites.”<sup>96</sup> In support of this statement, Mr. Hochman makes numerous speculative assertions without providing any analysis or supporting evidence regarding feasibility of these changes or their impact on usability of the Chrome browser, or potential second-order effects of such changes on other aspects of the market, business, and technology. Mr. Hochman also fails to consider the impact to users if all communications to Google were blocked in Incognito Mode.

---

<sup>93</sup> Brynjolfsson, Erik and Joo Hee Oh, “The Attention Economy: Measuring the Value of Free Digital Services on the Internet,” *Thirty Third International Conference on Information Systems, Orlando 2012*, 2012, available at <https://perma.cc/E2TZ-A6J9>.

<sup>94</sup> Greenwood, Jeremy et al., “‘You Will’: A Macroeconomic Analysis of Digital Advertising,” *Economics of Digital Services @ Penn*, 2021, available at <https://perma.cc/ZX8P-9LC2>.

<sup>95</sup> Hochman Report, Appendix A, ¶ 31.

<sup>96</sup> Hochman Report, ¶ 5.

73. As an initial matter, in asserting that Chrome should be redesigned to “either stop or limit” all transmissions of At-Issue Data to Google when a user visits a website in Incognito Mode, Mr. Hochman assumes that this is what users actually want. As described in my opening report, Private Browsing Modes, including Incognito Mode, are not designed to provide complete anonymity from websites that the user visits and third-party services that these websites have chosen to embed.<sup>97</sup> Mr. Hochman’s assertion to the contrary—that Incognito Mode should be designed to prevent Chrome from sending all messages to third-party web services—is not realistic because it ignores the stark negative impact this would have on users. For example, Google provides a number of services like the Google Fonts and Google Maps APIs that are used by numerous websites. Those services are enabled by transmissions to Google-associated domains that necessarily include fields such as IP addresses and user agent strings. If Chrome blocked all such transmissions in Incognito Mode as Mr. Hochman contends, websites would not be able to render the fonts provided by the Fonts API, or display the maps provided by the Maps API, which would negatively impact the experience of users visiting those websites.<sup>98</sup> In offering his opinion on this subject, Mr. Hochman ignores these impacts on the user’s browsing experience.

74. Mr. Hochman also relies on selected statements by current and former Google employees that he takes out of context. For example, Mr. Hochman argues that Google could have blocked third-party cookies by default before 2020, relying on the following testimony from former Google Engineer Justin Schuh: “So when you ask me if Google could technically block third-party cookies on – at any point in the history – like, could Chrome had launched without

---

<sup>97</sup> Zervas Affirmative Report, ¶ 43.

<sup>98</sup> See **Appendix E** for an illustration.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

third-party cookies, the answer is technically, yes.”<sup>99</sup> However, Mr. Hochman fails to include Mr. Schuh’s statements immediately preceding this statement (“[T]he hard part is the way that the technical change impacts everything else”) and immediately following it (“No one would have ever used it because it would have been a broken browser”).<sup>100</sup>

75. Mr. Hochman also mischaracterizes testimony of Google engineer Michael Kleber and product manager Abdel Karim Mardini on the subject of deletion of Incognito Mode session data on Google’s servers. Mr. Hochman quotes from Mr. Kleber’s deposition testimony to claim that Google never implemented a proposal whereby “[s]erver-side logs will be initially anonymized and then removed at the end of the Incognito session when the user enables this feature.”<sup>101</sup> However, Mr. Hochman fails to include Mr. Kleber’s remarks on the hypothetical nature of the proposal: “[S]ince the servers don’t actually do the thing being described here, the [proposal for] how should Chrome interact with servers that do the thing is a purely hypothetical question because the servers don’t actually do the thing being described.”<sup>102</sup>

76. Mr. Hochman further mischaracterizes Mr. Kleber’s testimony about proposals to “introduce anti-tracking features—including invasive anti-fingerprinting measures” and to mask IP addresses.<sup>103</sup> With regard to anti-tracking features, Mr. Hochman fails to include the following from Mr. Kleber: “I think there were a range of options where deploying [privacy-improving technologies] in Incognito Mode as described here is one option. And another option is deploying this range of protections for everybody, like making it a standard part of Chrome, whether you’re

---

<sup>99</sup> Hochman Report, ¶ 125.

<sup>100</sup> Deposition of Justin Schuh, January 6, 2022, p. 148:12-13, 19-20.

<sup>101</sup> Hochman Report, ¶ 126.

<sup>102</sup> Deposition of Michael Kleber, March 18, 2022 (“Kleber Deposition”), p. 20:16-20.

<sup>103</sup> Hochman Report, ¶¶ 128-129.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

in Incognito Mode or not. That second option is the one we ultimately landed on.”<sup>104</sup> Mr. Kleber described this as “one of the cornerstones of the Privacy Sandbox effort” that he is involved in.<sup>105</sup> With respect to IP address masking, Mr. Hochman fails to include the following from Mr. Kleber: “There are hard problems that need solving when you -- when you try to add IP privacy. There are things that IP addresses are used for, and if you add IP privacy blindly, then there are a lot of problems that you could cause. So there are many people, both inside of Google and outside of Google, who quite rightly urge caution to avoid accidentally breaking some important parts of the web or of the Internet by adding IP privacy without considering all of the potential consequences.”<sup>106</sup>

77. Similarly, Mr. Hochman cites testimony by former Google product manager Rory McClelland to argue that Google could have built a toggle to let users decide whether to signal to Google that they are browsing in Incognito Mode.<sup>107</sup> But Mr. Hochman ignores Mr. McClelland’s further testimony about the arguments against such a toggle, including web standards surrounding Private Browsing Modes, which provide that the “web server should be oblivious to the user’s private browsing intent, Chrome or otherwise.”<sup>108</sup>

78. I also find Mr. Hochman’s comparisons between Chrome and other browsers misleading. He uses tracking prevention features in Firefox and Safari as examples of what Google could implement in Chrome, but he ignores that Google provides several settings and extensions (e.g., the Google Analytics Opt-out extension) for users who want to block analytics and

---

<sup>104</sup> Kleber Deposition, p. 28:3-11.

<sup>105</sup> Kleber Deposition, p. 28:11-12.

<sup>106</sup> Kleber Deposition, p. 51:10-21.

<sup>107</sup> Hochman Report, ¶ 131.

<sup>108</sup> Deposition of Rory McClelland, February 18, 2022, p. 91:18-20.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

advertising communications on their Chrome browser. Mr. Hochman also compares Chrome’s Incognito Mode with Safari’s Private Browsing Mode, noting that “Safari’s Private Browsing mode was designed to not share cookies across all open windows and tabs.”<sup>109</sup> However, Mr. Hochman neglects to mention that Firefox, for example, has a Private Browsing Mode that operates in the same way as Chrome’s Incognito Mode in this respect. Similar to Chrome’s documentation, Mozilla also clarifies the features included in Firefox’s Private Browsing Mode in a page titled “Private Browsing - Use Firefox without saving history.”<sup>110</sup> The article states that, “[c]ookies set in private windows are held temporarily in memory, separate from regular window cookies, and discarded at the end of your private session (after the last private window is closed).”<sup>111</sup>

79. My review of the sources Mr. Hochman cites indicates that Google has considered a number of possible changes in the past, including some hypothetical changes that presented a number of technical hurdles. Mr. Hochman’s conclusion that Google could have designed Chrome’s Incognito Mode differently is speculative, ignores the negative impact these changes would have on users, and is based on selective quotations from witness testimony discussing these possible changes, while ignoring other testimony about their speculative nature and associated technical hurdles. Nor does he acknowledge the changes that Google actually implemented and

---

<sup>109</sup> Hochman Report, ¶ 163.

<sup>110</sup> “Private Browsing - Use Firefox without saving history,” *Mozilla Support*, available at <https://perma.cc/X9NG-QCB8>.

<sup>111</sup> “Private Browsing - Use Firefox without saving history,” *Mozilla Support*, available at <https://perma.cc/X9NG-QCB8>.

continues to work toward implementing, for which there is abundant information available to the public.<sup>112</sup>

#### **IV. REBUTTAL TO MR. HOCHMAN’S ASSERTIONS REGARDING USER AND WEBSITE NOTIFICATIONS**

##### **A. Mr. Hochman’s Opinions Regarding User Notification And Choice Are Flawed (Hochman Opinion 5)**

80. In his Opinion 5, Mr. Hochman asserts that Google “intercepted private browsing communications without notifying users or providing a choice at the time of collection,” and that Google “could have provided such a notification but did not.”<sup>113</sup> Mr. Hochman further states that “[w]hen visiting a non-Google website containing Google tracking beacons in a private browsing mode, users are not notified of the Google tracking beacons or Google’s collection of private browsing information or given a choice regarding that collection.”<sup>114</sup> These statements are flawed for several reasons.

81. First, as I discuss in my opening report, when a user opens a Private Browsing Session in any major browser, the Splash Screen informs the user what Private Browsing Mode is and what it is *not*.<sup>115</sup> For example, in the case of Incognito Mode, users are informed that the user’s activity will still be visible to websites, employers or school, and internet service providers.<sup>116</sup> The

---

<sup>112</sup> See e.g., “Protecting your privacy online,” *The Privacy Sandbox*, Google, available at <https://perma.cc/C2TM-927B>; and “Google Chrome,” *The Keyword*, Google, available at <https://perma.cc/5QFA-CBFC>.

<sup>113</sup> Hochman Report, ¶ 6.

<sup>114</sup> Hochman Report, ¶ 134.

<sup>115</sup> Zervas Affirmative Report, Section IV.B.

<sup>116</sup> Zervas Affirmative Report, ¶ 50.

Incognito Splash Screen also contains a link to more detailed descriptions of Incognito Mode, as I also discuss in further detail in my opening report.<sup>117</sup>

82. Second, Mr. Hochman ignores that Google’s policies require websites using Google’s services to provide notice to users about the website’s collection of data. For example, Google Analytics policies state that websites are responsible for:

- ***User notification:*** “You must give your end users proper notice about the implementations and features of Google Analytics that you use, including notice about what data you will collect via Google Analytics, and whether this data can be connected to other data you have about the end user. You must obtain consent from your end users, or otherwise provide them with the opportunity to opt-out from the implementations and features you use.”<sup>118</sup>
- ***Types of data transmitted to Google:*** “You must not upload any data that allows Google to personally identify an individual (such as certain names, Social Security Numbers, email addresses, or any similar data), or data that permanently identifies a particular device (such as a unique device identifier if such an identifier cannot be reset).”<sup>119</sup>

---

<sup>117</sup> Zervas Affirmative Report, ¶ 52.

<sup>118</sup> “Measurement Protocol, SKD, and User ID Feature Policy,” *Google Analytics*, Google, available at <https://perma.cc/88W2-LDYD>.

<sup>119</sup> “Measurement Protocol, SKD, and User ID Feature Policy,” *Google Analytics*, Google, available at <https://perma.cc/88W2-LDYD>.

83. Similarly, Google Ad Manager’s policies for publisher websites clearly state that publisher websites must inform users about any data sharing that occurs as part of using Google Ad Manager:

“Publishers must: have and abide by a privacy policy that clearly discloses any data collection, sharing and usage that takes place on any site app, email publication of other property as a consequence of your use of Google products. The privacy policy must disclose to users that third parties may be placing and reading cookies on your users’ browsers or using web beacons to collect information as a result of ad serving on your website.”<sup>120</sup>

84. Additionally, Google Ad Manager’s policies state that publishers must “not pass any information to Google data that Google could use or recognize as personally identifiable information; or that permanently identifies a particular device.”<sup>121</sup>

85. Third, Mr. Hochman claims that based on his review of the top 25 websites for Google Analytics and the top 25 websites for Google Ad Manager as well as a number of other websites he visited “none of those websites had any such pop-up notification – or any process by which users would be informed that Google would collect and exploit their private browsing information.”<sup>122</sup> This assertion is inaccurate. When I visited the same websites in Private Browsing Mode, I found that all provided notices to users about data collection, many including specific references to Google services, and did not indicate or suggest that this data collection would stop

---

<sup>120</sup> “Google Publisher Policies: Privacy-related policies: Privacy disclosures,” *Google Ad Manager Help, Google*, available at <https://perma.cc/G2FU-Z7PK>.

<sup>121</sup> “Google Publisher Policies: Privacy-related policies: Privacy disclosures,” *Google Ad Manager Help, Google*, available at <https://perma.cc/G2FU-Z7PK>.

<sup>122</sup> Hochman Report, ¶ 134.



when a user browses in a Private Browsing Mode.<sup>123</sup> For example, the following websites disclose data collection in general to users:

- ***LinkedIn.com***: “As further described in our Cookie Policy, we use cookies and similar technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your device(s) on, off and across different services and devices where you have engaged with our Services.”<sup>124</sup>
- ***Businessinsider.com***: “We use cookies for a variety of reasons. Cookies make it easier for you to log on to and use the Sites during visits. The aggregate information collected permits us to analyze traffic patterns and target the interests of our users. This helps us provide you with a better experience by improving the content and making our Sites easier to use. [...] Web beacons allows us, for example, to monitor how users move from one page within our Sites to another, to track access to our communications, to understand whether users have come to our Sites from an online advertisement displayed on a third-party website, to measure how ads have been viewed and to improve site performance. [...] Please note that third parties (including, for example, advertising networks and providers of external services like web traffic analysis services) use cookies, over which we have no control. These cookies are likely to be analytical/performance cookies or targeting cookies.”<sup>125</sup>

---

<sup>123</sup> **Appendix D** includes the list of the websites that were not accessible for review and screenshots for the websites highlighted in my report. My backup materials include the review of privacy notices for all accessible websites.

<sup>124</sup> “Privacy Policy,” *LinkedIn*, August 11, 2020, available at <https://perma.cc/2TT8-37Q2>.

<sup>125</sup> “Cookies Policy,” *Insider Inc.*, September 4, 2019, available at <https://perma.cc/MH9H-5V3Z>.

- ***Washingtonpost.com***: “We and our service providers may use cookies, web beacons, and other tracking technologies to collect such information.”<sup>126</sup>

86. I also found many examples that explicitly inform users that the websites use Google Analytics. For example:

- ***Change.org***: “We use third-party analytics services like Google Analytics provided by Google Inc. (“Google”), the Amplitude service provided by Amplitude (“Amplitude”), the Optimizely service provided by Optimizely (“Optimizely”), and the Chartio service provided by Chartio (“Chartio”). These analytics services may use cookies and similar technologies to analyze how people use our services and provide statistical reports about aggregate user behavior.”<sup>127</sup>
- ***Grammarly.com***: “These cookies track information about your visits and usage of the Site, Software, and/or Services so that we can make improvements and report our performance — for example, to analyze visitor and user behavior so as to provide more relevant content or suggest certain activities. We might also use analytics cookies to test new ads, pages, or features to see how users react to them. Google Analytics is the main technology we currently use in this regard.”<sup>128</sup>
- ***Privy.com***: “Please note in particular that we may use Google Analytics and other similar services. Google Analytics uses cookies to help analyze how users use the Site. The information generated by the cookie about your use of the Site (including your IP address) will be transmitted to and stored by Google, Inc. (“Google”). Google may use

<sup>126</sup> “Privacy Policy,” *The Washington Post*, October 5, 2021, available at <https://perma.cc/5WVW-YRQV>.

<sup>127</sup> “Privacy Policy,” *Change.org*, March 25, 2022, available at <https://perma.cc/G2HG-5AEV>.

<sup>128</sup> “Cookie Policy,” *Grammarly*, December 30, 2019, available at <https://perma.cc/V5MQ-G8B9>.

this information for the purpose of evaluating your use of the Site, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage.”<sup>129</sup>

87. Further, some websites such as *accuweather.com* also mention the use of ad-related services such as DoubleClick:<sup>130</sup>

“AccuWeather and third-party vendors, including Google, may use first-party cookies (such as the Google Analytics cookies) and third-party cookies (such as the DoubleClick cookie) together to: (a) inform, optimize and serve ads based on a user's past visits to AccuWeather Sites or (b) report how Your ad impressions, other uses of ad services, and interactions with these ad impressions and ad services are related to visits to AccuWeather Sites.”<sup>131</sup>

88. I have tested and confirmed that the website notifications described above are accessible to users in Private Browsing Mode in each of the Chrome, Safari, and Edge browsers.<sup>132</sup> In other words, if someone visits these websites using a Private Browsing Mode of any of the Chrome, Safari, or Edge browsers, these websites’ privacy notifications are accessible to the user.

89. Mr. Hochman also ignores that there are websites that display pop-up notifications to users in Incognito Mode informing them of the site’s use of Google Services. As I described in my opening report, the Latham and Watkins LLP websites (*lw.com*) shows a pop-up notification that immediately asks users, irrespective of the browsing mode, whether they consent to the use of Google Analytics as illustrated in **Figure 6**.<sup>133</sup>

<sup>129</sup> “Privacy Policy,” *Privy*, December 20, 2019, available at <https://perma.cc/A8HS-5M6E>.

<sup>130</sup> “Privacy Policy,” *AccuWeather*, August 21, 2020, available at <https://perma.cc/4NT5-WCHW>.

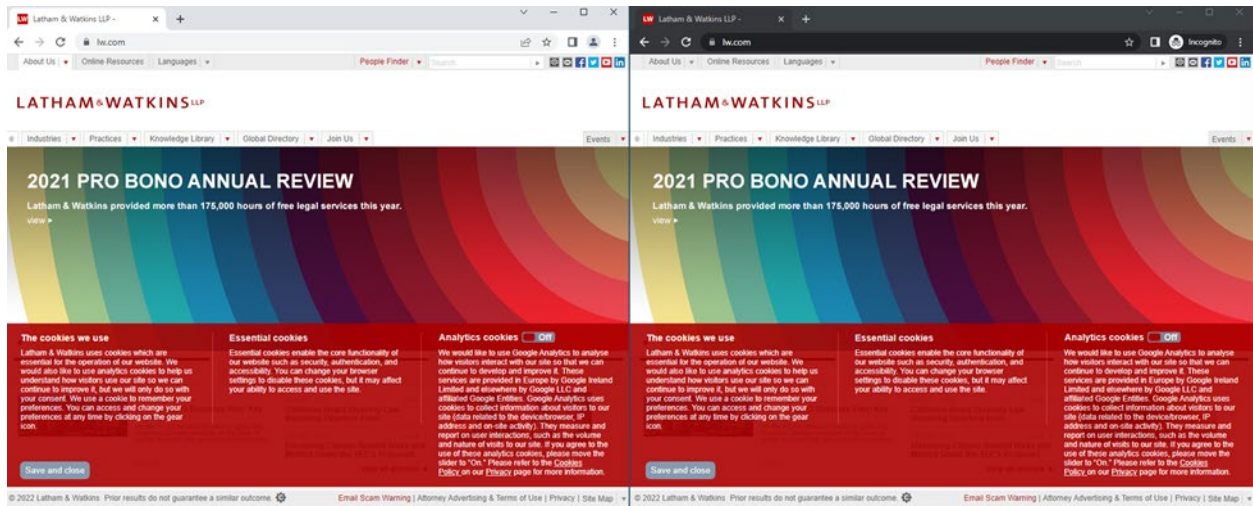
<sup>131</sup> “Privacy Policy,” *AccuWeather*, August 21, 2020, available at <https://perma.cc/4NT5-WCHW>.

<sup>132</sup> See **Appendix D** for screenshots.

<sup>133</sup> Zervas Affirmative Report, ¶ 96.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure 6**  
**Latham & Watkins LLP Pop-Up Notification Example**



90. In asserting that Google did not provide users a choice, Mr. Hochman also neglects that users have a variety of settings and extensions that affect whether At-Issue Data flows to third-party services embedded in websites that the users visit.<sup>134</sup> I also performed tests discussed in my opening report and confirmed that these options function as advertised and restrict transmissions of At-Issue Data to Google.<sup>135</sup> For example, users can block or limit execution of third-party code using built-in browser settings or external extensions. Further, as I also discuss in my opening report, these settings and extensions are applicable in both Regular and Private Browsing Modes, although users may need to enable extensions in Private Browsing Mode.<sup>136</sup> Based on these settings that give users control over transmissions of At-Issue Data to Google when they visit a website that uses a Google service, I disagree with Mr. Hochman's assertion that users are not given a choice in relation to the transmissions of At-Issue Data in this case.

<sup>134</sup> Zervas Affirmative Report, Sections V.A.2 and V.B.2.

<sup>135</sup> Zervas Affirmative Report, Section V.D.

<sup>136</sup> Zervas Affirmative Report, ¶ 118.

91. I also disagree with Mr. Hochman’s assertion that Google could have provided a notification or offered a choice to users “at the time of collection.”<sup>137</sup> This assumes that Google can identify whether a user is in a Private Browsing Mode in Chrome or another browser when they visit a website that uses Google’s services; however, as I discuss in **Section IV.B** below, Private Browsing Modes are intended to not be detectable to websites or their third-party web-service providers. Additionally, Mr. Hochman provides no explanation as to how Google would notify users of non-Google browsers such as Safari or Edge “at the time of collection.”

**B. Mr. Hochman’s Opinions Regarding Notifications To Websites Are Flawed (Hochman Opinion 6)**

92. In his Opinion 6, Mr. Hochman claims that Google “intercepted private browsing communications without notifying websites or providing a choice at the time of collection.”<sup>138</sup> This claim is flawed as it assumes that website owners were unaware of how Private Browsing Modes operate in relation to the third-party services upon which they rely.

93. Mr. Hochman’s assertions that websites were not aware of how Private Browsing Mode operates is also contradicted by the fact that websites have expressed concerns about the lack of ability to detect Private Browsing Mode users. For example, news websites such as *The New York Times* have in the past developed strategies to detect (and block) Private Browsing Mode users who could use that browser feature to bypass paywalls.<sup>139</sup> *The New York Times* business

---

<sup>137</sup> Hochman Report, ¶ 135.

<sup>138</sup> Hochman Report, ¶ 7.

<sup>139</sup> Benton, Joshua, “Your favorite way to get around The New York Times paywall might be about to go away,” *NiemanLab*, February 28, 2019, available at <https://perma.cc/F5ED-BV3H>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

model relies on revenues from both subscription and ads channels.<sup>140</sup> Users must buy a subscription to access all content, but users may view a limited number of articles for free. The limit to the number of articles was enforced through the placement of cookies, which allowed *The New York Times* to detect how many articles had recently been viewed from that browser and thus whether the limit was reached. However, since each Private Browsing Session started without any cookies set, visitors in a Private Browsing session would appear to *The New York Times* website to be first-time visitors. This allowed Private Browsing Mode users to bypass the limit on viewing free articles. In response, *The New York Times* developed methods to detect if a website visitor was in a Private Browsing Mode and reimpose the limit of free articles. This example illustrates that websites like *The New York Times* developed methods *precisely* because they were aware that Chrome and other browsers do not reveal the Private Browsing Mode status of a website visitor and how Private Browsing Modes operate. In response to the workarounds to identify whether a website user was in Incognito Mode, Google implemented numerous updates to Chrome to limit the ability of websites to detect Incognito Mode.<sup>141</sup>

94. It is well known in the industry that Private Browsing Modes are designed not to inform websites of users' private browsing status. For example, as described in **Section III.A** above the W3C states that browser vendors should design private browsing modes so that they work in a way that is "indistinguishable" for websites from normal browsing mode.<sup>142</sup> Based on

---

<sup>140</sup> Zacks Equity Research, "Subscription Revenues a Key Driver for NY Times (NYT) in 2022," *Yahoo*, December 21, 2021, available at <https://perma.cc/BGY8-EHW7>.

<sup>141</sup> Bradshaw, Kyle, "Google wants to make it harder for sites to detect that you're using Chrome's Incognito Mode," *9to5Google*, February 15, 2019, available at <https://perma.cc/QSX5-J6RV>.

<sup>142</sup> "W3C TAG Observations on Private Browsing Modes," World Wide Web Consortium, April 9, 2020, available at <https://perma.cc/8SLY-NZ66>.

these public discussions, I expect that website developers are aware that browsers do not identify whether a user is in Regular or Private Browsing Mode.

95. In addition, as I discuss in my opening report, Google’s public documentation about its Analytics service also provides an extensive description of how the service works.<sup>143</sup> For example, public documentation describes how websites can enable Google Analytics services<sup>144</sup> and which data can be sent to Google.<sup>145</sup> Notably, I did not find any information in Google Analytics public documentation that suggests that Google Analytics operates differently in Private Browsing Modes. In fact, public documentation implies that Google Analytics operates in Private Browsing Mode. For example, it explains that “[d]ifferent web browsers on the same device, including instances of incognito and private browsing, are counted as unique devices in the Cross Device reports.”<sup>146</sup> Thus, based on this publicly available Google document, I expect that Google Analytics customers are aware that the service will attempt to collect information regarding users’ visits to the customer’s websites, whether or not they do so in Private Browsing Mode.

96. Additionally, it is a common practice to test websites in Private Browsing Modes to see how websites behave when “things like cookies and temp files are not saved.”<sup>147</sup> Mr. Hochman has not identified, and I have not seen, any evidence indicating that website developers are not aware that third-party services such as Google’s analytics and advertising

---

<sup>143</sup> See, Zervas Affirmative Report, Section V.A.

<sup>144</sup> See e.g., Zervas Affirmative Report, ¶ 88.

<sup>145</sup> See e.g., Zervas Affirmative Report, ¶ 90.

<sup>146</sup> “Limits of User-ID view & Cross Device reports,” *Analytics Help, Google*, available at <https://perma.cc/BAM5-AYUB>.

<sup>147</sup> “Strategies for carrying out testing,” *MDN Web Docs*, available at <https://perma.cc/F5G6-KN2C>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

services will operate in Private Browsing Modes similarly to how they operate in Regular Browsing Modes.<sup>148</sup>

## **V. REBUTTAL TO MR. HOCHMAN’S ASSERTIONS REGARDING USER PROFILES (HOCHMAN OPINION 10)**

97. In his Opinion 10, Mr. Hochman states that “Google, throughout the class period, created detailed profiles tied to various Google identifiers (that remain undisclosed to users) based on the private browsing information it collected.”<sup>149</sup> This statement is flawed as Mr. Hochman ignores that analytics and advertising cookie values sent in Private Browsing Sessions are different from those in Regular Mode Sessions or different Private Mode Sessions, and the cookie values from Private Browsing Sessions cannot be used as a link to the user or her device after the session is closed.

98. The “detailed profiles” Mr. Hochman describes are in fact “orphaned” islands of data reflecting browsing activity from just one Private Browsing Session. The data are associated only with a cookie value that is deleted from the user’s browser when she closes the Private Browsing Session.<sup>150</sup> For users who do not sign into their Google Accounts (as the class members here), the cookie values set in Private Browsing Mode cannot be used to link the user’s activities in a given Private Browsing Session to the user’s activities in other Regular or Private Browsing Sessions.<sup>151</sup> This prevents Google from using these cookie values to create a “cradle-to-grave

---

<sup>148</sup> As noted in my opening report, Private Browsing Modes restrict certain functionality such as access to cookies and other information from other browser sessions and depending on the browser might block third-party cookies.

<sup>149</sup> Hochman Report, ¶ 11.

<sup>150</sup> Zervas Affirmative Report, ¶¶ 80-84.

<sup>151</sup> In my opening report, I conducted systematic testing of whether cookies are shared between Regular and Private Browsing Sessions for popular browser and operating system combinations. For all testing



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

profile of users,” as Plaintiffs allege.<sup>152</sup> Rather, the purported “profiles” based on cookie values, to which Mr. Hochman refers, reflect at most certain browsing activity (visits to websites that use Google services) by an unidentified user during a single Private Browsing Session.

## **VI. REBUTTAL TO MR. HOCHMAN’S ASSERTION THAT GOOGLE CIRCUMVENTED COOKIE BLOCKERS AND ANTI-TRACKING MEASURES (HOCHMAN OPINION 15)**

99. In his Opinion 15, Mr. Hochman asserts that Google attempted “to circumvent efforts by other companies to block Google tracking beacons.”<sup>153</sup> As support for this opinion, Mr. Hochman refers to certain features of Google products that he contends circumvent such technologies as Firefox Private Browsing or Apple’s Intelligent Tracking Prevention. However, Mr. Hochman’s assertion rests on an incomplete basis and fails to acknowledge various aspects of how these Google products function and the purpose they serve.

### *1. PPID*

100. Based on each of the factors described below, I disagree with Mr. Hochman’s broad statements that PPID works to circumvent efforts by other companies to block Google tracking beacons. Instead, PPID is an example of Google providing a feature to publishers that is allowed by the Firefox and Apple technologies to which Mr. Hochman refers.

---

variations, I observed that cookie values stored from prior Regular Mode Sessions are not used in Private Browsing Sessions. Similarly, cookie values set in Private Browsing Session are not carried over to subsequent Regular or Private Browsing Sessions. As a result, these cookie values cannot be used to link the Private Browsing Mode activities to a user or her device after that Private Browsing Session is closed. See, Zervas Affirmative Report, Section IV.C.

<sup>152</sup> Third Amended Class Action Complaint, Chasom Brown, et al., v. Google LLC, United States District Court Northern District of California, February 3, 2022 (“Complaint”), ¶ 93.

<sup>153</sup> Hochman Report, ¶ 16.

101. First, Mr. Hochman asserts that “[w]ith the loss of certain Google cookies (e.g., due to blocking of certain Google cookies based on Apple’s Intelligent Tracking Prevention (‘ITP’) or Google’s [REDACTED] changes to Chrome Incognito Mode), Google mitigates targeting loss by relying on first-party identifiers, such as the PPID available for Google Ad Manager 360 Publishers.”<sup>154</sup> Mr. Hochman asserts that “[t]his identifier is used to identify users that log into publisher websites, and it uniquely identifies a user across all of the user’s devices, browsers, and browsing sessions, including private browsing sessions.”<sup>155</sup> This is incorrect. PPID is not used to uniquely identify a user across all of their devices, browsers, and browsing sessions. To the contrary, PPID is used for “ad frequency capping, audience segmentation, and other delivery controls across devices,” as I explained in my opening report.<sup>156</sup> Mr. Hochman’s description ignores the fact that PPIDs are first-party identifiers that are not shared among publishers.<sup>157</sup> Thus, if a user were to sign into two different publishers’ websites, even if those publishers both used PPID, the user would not have the same PPID between the two websites. Thus, PPID does not enable a user to be tracked between websites of different publishers and does not serve the same purpose as a third-party cookie.

102. Second, Mr. Hochman fails to consider that PPID is also conditional on websites deciding to use it.<sup>158</sup> Therefore, availability of the PPID to Google depends on (a) a user visiting the website of a publisher that uses PPID; (b) the publisher assigning a PPID for that user, e.g.,

---

<sup>154</sup> Hochman Report, ¶ 187.

<sup>155</sup> Hochman Report, ¶ 187.

<sup>156</sup> Zervas Affirmative Report, ¶ 110.

<sup>157</sup> “About publisher provided identifiers,” *Ad Manager Help*, Google, available at <https://perma.cc/P6WG-YX4S>.

<sup>158</sup> Hochman Report, ¶ 187.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

when the user signs in to the website; and (c) the publisher deciding to share the PPID with Google. On the last point, if a publisher decides not to share these with Google, these identifiers will not appear anywhere on Google’s systems.<sup>159</sup>

103. Third, as explained in public Google documentation describing “How PPIDs Work,” “the identifier sent to Ad Manager must be hashed or encrypted such that it is meaningless to Google, and it must not be raw personally identifiable information, a raw third-party ID, or a raw device ID.”<sup>160</sup> Therefore, PPID values do not include information that can link to a users’ identity.

104. Fourth, Google requires that users have a way to opt out of personalized ads and blocks the use of PPID for users who choose to do so. If Google detects that a user has opted out of personalized ads, “features permitting the use of PPID for targeting ads to the user’s web browser will be disabled.”<sup>161</sup>

105. Based on the aspects of the PPID features described above, I do not agree that it is a replacement for third-party cookies or that its use circumvents third-party cookie blockers or any other privacy-oriented features of the Firefox and Apple technologies to which Mr. Hochman refers.

---

<sup>159</sup> Zervas Affirmative Report, ¶ 110.

<sup>160</sup> “About publisher provided identifiers,” *Ad Manager Help, Google*, available at <https://perma.cc/P6WG-YX4S>.

<sup>161</sup> “About publisher provided identifiers,” *Ad Manager Help, Google*, available at <https://perma.cc/P6WG-YX4S>.

## 2. *Enhanced Conversions*

106. Mr. Hochman also offers several incorrect statements regarding “Enhanced Conversions in Analytics and Ads,” which he asserts allow non-Google websites to “send personally identifying information such as a user’s email address (user’s name, home address, and phone number may also be used) to Google to be matched against the same user’s Google account information containing the same identifying information.”<sup>162</sup> In my opinion, this is incorrect at least because it suggests that this happens to every user. As described in public documentation, enhanced conversion functionality can only be used if a user is signed into Google when they engage with an ad,<sup>163</sup> and also requires that the user enter information (such as an email or a phone number) on the advertiser website.<sup>164</sup> For instance, the enhanced conversions feature could measure a conversion only if a Google signed-in user engages with an ad, then visits the advertiser’s website and enters their email address in the advertiser’s website (assuming the advertiser utilizes the enhanced conversions feature).

107. Mr. Hochman’s assertions regarding enhanced conversions are also misleading because, similar to PPID, before enhanced conversion data are sent to Google data are processed by a hashing algorithm that masks user data.<sup>165</sup> Google summarizes the enhanced conversion functionality as “[w]ith enhanced conversions for web, first-party customer data such as an email address, name, home address, or phone number is captured in your conversion tracking tags, hashed, sent to Google in its hashed form, and then used to match your customers to Google

---

<sup>162</sup> Hochman Report, ¶ 209.

<sup>163</sup> “About enhanced conversions,” *Google Ads Help, Google*, available at <https://perma.cc/6UH8-9Q7X>.

<sup>164</sup> “Set up enhanced conversions for web manually with Google Tag Manager”, *Google Ads Help, Google*, available at <https://perma.cc/CR99-8WUE>.

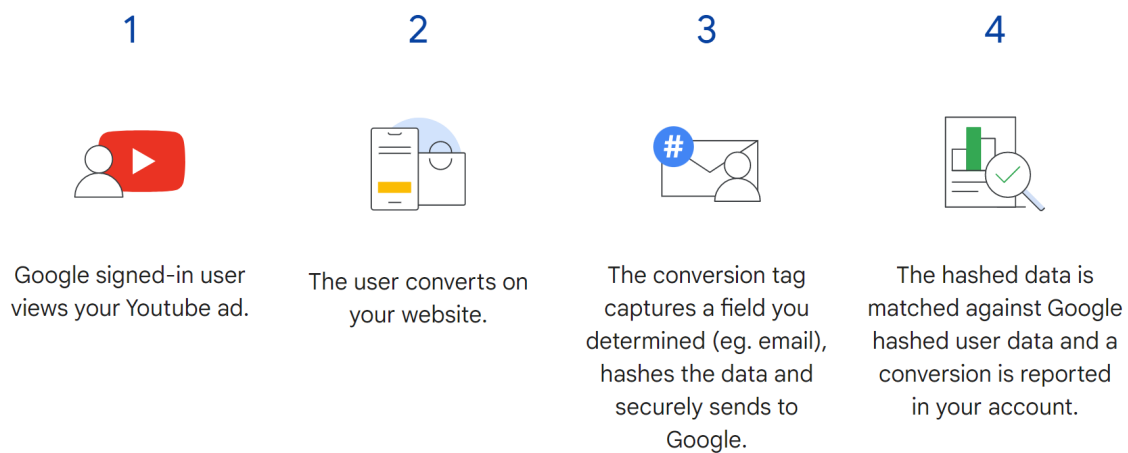
<sup>165</sup> “About enhanced conversions,” *Google Ads Help, Google*, available at <https://perma.cc/6UH8-9Q7X>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

accounts, which were signed-in to when they engaged with one of your ads.” The process of how enhanced conversion operates is also illustrated in **Figure 7** below:<sup>166</sup>

**Figure 7**  
**Enhanced Conversion Flow**

### Enhanced conversions for web



108. Based on the aspects of the enhanced conversion feature described above, I do not agree that it is a replacement for third-party cookies or that its use circumvents third-party cookie blockers or any other privacy-oriented features of the Firefox and Apple technologies to which Mr. Hochman refers.

<sup>166</sup> “About enhanced conversions,” *Google Ads Help*, Google, available at <https://perma.cc/6UH8-9Q7X>.

**VII. REBUTTAL TO MR. HOCHMAN’S OPINIONS REGARDING IMPACT ON USERS (HOCHMAN OPINIONS 26 THROUGH 28)**

109. Mr. Hochman asserts three opinions related to his claims that “Google’s attempted interception and collection uniformly impacted all class members.”<sup>167</sup> In his Opinion 26, he asserts that Google “uniformly attempted to intercept all private browsing communications with non-Google websites that have a Google tracking beacon—regardless of which private browsing mode the user employed.”<sup>168</sup> In his Opinion 27, Mr. Hochman asserts that “Google’s tracking beacons were so ubiquitous throughout the class period that there is a near certainty that almost every person using the private browsing modes at issue [...] had their private browsing information intercepted by Google, including while visiting non-Google websites without being signed into any Google account.”<sup>169</sup> In his Opinion 28, Mr. Hochman asserts that “Google does not offer users any control to escape Google’s tracking beacons,” which according to Mr. Hochman are “almost impossible to avoid.”<sup>170</sup> As described below, these statements are incorrect.

110. Mr. Hochman asserts that “Google’s attempted interception and collection uniformly impacted all class members,”<sup>171</sup> and that “Google designed its tracking and advertising code to be embedded on any website and to be agnostic to the specific browser and device for web browsing.”<sup>172</sup> I disagree with these assertions. As detailed in my opening report and further described herein, there are multiple browser settings and extensions available to users that will affect transmissions of At-Issue Data to Google when the user visits a website that makes use of

---

<sup>167</sup> Hochman Report, Section VIII.I.

<sup>168</sup> Hochman Report, ¶ 27.

<sup>169</sup> Hochman Report, ¶ 28.

<sup>170</sup> Hochman Report, ¶ 29.

<sup>171</sup> Hochman Report, Section VIII.I.

<sup>172</sup> Hochman Report, ¶ 308.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Google’s analytics or advertising services. The tags that Google makes available to websites that choose to use those services are also configurable, and there are multiple settings available to those websites that also affect transmissions of At-Issue Data to Google. As a result, to the extent there is an “impact” on purported class members of the transmissions of At-Issue Data in this case, I do not agree that any such impact is “uniform” to all class members, as Mr. Hochman contends.

111. Mr. Hochman further asserts that “Google does not provide users with any tool to escape these Google ‘tracking beacons’ on non-Google websites.”<sup>173</sup> This is incorrect, too. Google and other browser vendors *do* provide tools to users that will affect the flow of At-Issue Data to Google. In Section V of my opening report, I summarized settings and extensions that allow users to change which data are transmitted to Google and other services. In my analysis, I tested the following tools that affect data flow: cookie blocking settings, JavaScript blocking settings and extensions, an extension that allows restricting Google Analytics data flow, and an extension that blocks advertising and other types of content. I found that these tools affect data transmissions of At-Issue Data to Google whether a user is in Regular or Private Browsing Mode.<sup>174</sup> Even though my analysis is focused on the Chrome browser using the Windows operating system, similar settings and extensions are available on other browsers and operating systems which makes my analysis generalizable to other cases.<sup>175</sup> The analysis presented in my report serves as an example and was not intended as an exhaustive list of settings and extensions that users can use that are

---

<sup>173</sup> Hochman Report, ¶ 312.

<sup>174</sup> Zervas Affirmative Report, Section V.

<sup>175</sup> See e.g., “Google Analytics Blocker,” *Firefox Browser Add-Ons*, available at <https://perma.cc/L3RX-X2A6>; Orgera, Scott, “How to Disable JavaScript in Firefox,” *Lifewire*, December 2, 2020, available at <https://perma.cc/5GLL-U868>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

available in all popular browsers. Some users do indeed use these tools.<sup>176,177</sup> Therefore, I disagree with Mr. Hochman that users cannot affect whether and how At-Issue Data are transmitted to Google while users are in Private Browsing Mode, and I disagree with Mr. Hochman that “there is a near certainty that almost every person” had their private browsing information transmitted to Google.

112. Mr. Hochman also states that “[t]he Plaintiffs in this case are alleging that Google portrayed private browsing mode, including Incognito mode, as the control to prevent Google from tracking them across non-Google websites.”<sup>178</sup> Other than reference to the Plaintiffs’ allegations, Mr. Hochman does not provide support for this assertion. As confirmed by the testing described in my opening report, and as stated in **Section VIII** of this report, Private Browsing Modes in Chrome and other browsers operate consistently with how Google describes their operation to users. Further, to the extent Mr. Hochman asserts that Incognito Mode does not provide any privacy protections to users, I disagree. Incognito Mode *does* provide a measure of control and privacy for the user. For example, as described in **Section VIII** of this report, in Incognito mode, cookies existing on the browser are not shared, and new cookies set during the Incognito Mode session are discarded at the end of the session. Therefore, cookies cannot be used to link the user’s activity in Incognito Mode with cookie values set in other sessions.

---

<sup>176</sup> Zervas Affirmative Report, ¶ 136.

<sup>177</sup> Schneier, Bruce, “Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,” W.W. Norton & Company, 2015, p. 40.

<sup>178</sup> Hochman Report, ¶ 312.



**VIII. REBUTTAL TO MR. HOCHMAN’S ASSERTIONS REGARDING HOW CHROME’S INCOGNITO MODE OPERATES (HOCHMAN OPINION 29)**

113. In his Opinion 29, Mr. Hochman claims that “Google’s Chrome Incognito mode functioned in ways that were different than represented.” Mr. Hochman further claims that “the Incognito Splash Screen represents that ‘Chrome won’t save the following information: Your browsing history, cookies and site data, information entered in forms.’ This statement is false as a technical matter.”<sup>179</sup> Mr. Hochman’s sole basis for saying that is that he claims “Chrome does save browsing history as well as cookies and site data within Incognito sessions—at a minimum for the duration of the Incognito session.”<sup>180</sup> I disagree with Mr. Hochman’s statements on these issues for several reasons.

114. First, Mr. Hochman’s assertion that data are saved for the duration of the Incognito Mode session is exactly how Google describes Incognito Mode in various publicly available documents.<sup>181</sup> Specifically, Mr. Hochman ignores descriptions from the “Learn More” page that is linked from the Incognito Mode Splash Screen. The “Learn More” page states that “When you first open a new Incognito window, you’re creating a new Incognito browsing session. Any Incognito windows you open after that are part of the same session. You can end that Incognito session by closing all open Incognito windows.”<sup>182</sup> Further, under the “What Incognito mode does” section, the “Learn More” page states that “[e]ach time you close all Incognito windows, Chrome

---

<sup>179</sup> Hochman Report, ¶ 320.

<sup>180</sup> Hochman Report, ¶ 320.

<sup>181</sup> Hochman Report, ¶ 320.

<sup>182</sup> “How Chrome Incognito keeps your browsing private,” *Google Chrome Help*, Google, available at <https://perma.cc/2YZX-VG2U>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

discards any site data and cookies associated with that browsing session.”<sup>183</sup> Further, the Chrome Privacy Notice states that “Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new cookies on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.”<sup>184</sup> Mr. Hochman’s description of how Incognito Mode operates is exactly how Google describes it.

115. Second, the tests I conducted and discussed in Section IV.C.2 of my opening report show that Private Browsing Modes, including Incognito Mode, prevent cookie values from being shared across browsing sessions. Chrome keeps cookie values associated with an individual Incognito Mode Session separate from cookie values set in other sessions, whether those are Incognito Mode or Regular Mode Sessions. My testing confirmed that cookie values set in a Regular Mode Session are not available in a Private Browsing Session, and cookie values set during a Private Browsing Session are not available in subsequent Regular Mode or Private Browsing Sessions. Further, my tests also show that users’ browsing history, website logins, and autofill web forms are discarded after a Private Browsing Session has ended.<sup>185</sup> My tests confirmed that Private Browsing Modes such as Incognito work as described to users. Mr. Hochman does not perform any tests that show otherwise. For example, Mr. Hochman did not perform any tests or identify any evidence showing that cookie values associated with Private Browsing Sessions are not discarded once the session is closed, or that Incognito Mode does not conceal a user’s browsing activity from other people who may use the same device.

---

<sup>183</sup> “How Chrome Incognito keeps your browsing private,” *Google Chrome Help*, Google, available at <https://perma.cc/2YZX-VG2U>.

<sup>184</sup> “Google Chrome Privacy Notice,” *Google*, September 23, 2021, available at <https://perma.cc/SX4Q-3YU4>.

<sup>185</sup> Zervas Affirmative Report, Section IV.A.

116. My tests also confirmed that Private Browsing Modes such as Incognito operate consistent with industry recommendations relating to private browsing. As noted by W3C<sup>186</sup> and discussed in my opening report,<sup>187</sup> “Privacy modes offer some layer of isolation from browsing in regular browsing mode. Specifically, state information (cookies, saved passwords, list of visited sites, and other forms of client-side storage) is not kept between browser sessions. This for example means that on-disk traces should not be retained by the browser between two sessions (which in some cases may potentially still be recovered by other means).”<sup>188</sup>

117. Third, Mr. Hochman asserts that “throughout the class period, Chrome Incognito mode did not sandbox individual windows and tabs. Instead, Google designed Chrome Incognito to function in a way where cookies were shared across all Incognito windows and tabs open at the same time.”<sup>189</sup> But this is exactly how Google describes Incognito Mode to users. For example, the “How Chrome Incognito keeps your browsing private” page states “Close all Incognito windows and tabs when you’re done browsing. You end a session when you close all Incognito windows, so closing a single tab won’t discard your data. If you see a number next to the Incognito icon on your desktop or at the bottom of your browser on a mobile device, you have more than one Incognito window or tab open.”<sup>190</sup>

---

<sup>186</sup> “W3C TAG Observations on Private Browsing Modes,” *World Wide Web Consortium*, April 9, 2020, available at <https://perma.cc/8SLY-NZ66>.

<sup>187</sup> Zervas Affirmative Report, Section IV.D.

<sup>188</sup> “W3C TAG Observations on Private Browsing Modes,” *World Wide Web Consortium*, April 9, 2020, available at <https://perma.cc/8SLY-NZ66>.

<sup>189</sup> Hochman Report, ¶ 162.

<sup>190</sup> “How Chrome Incognito keeps your browsing private,” *Google Chrome Help*, Google, available at <https://perma.cc/2YZX-VG2U>.

118. Finally, to support these arguments, Mr. Hochman provides an incomplete quote from a former Google engineer, Rory McClelland, in which he omits the text in bold below:

“I would argue that we do store it, just in memory only. One of main misunderstanding (sic) we have with IM is with people not closing their sessions, which would be reasonable if they believed we never store the data. **'Storage' is different from writing to disk, in my opinion at least. Whilst this doesn't make much difference at the local level,** it does have an impact on the accumulation of cookies (and sign-ins) that allow the user to be tracked, even in Incognito mode.”<sup>191</sup>

119. Mr. McClelland’s testimony indicates that there is a distinction between Chrome storing data temporarily in memory versus writing data to disk. I agree. Browsers can store information in temporary memory to enable the browser to function—for example, when a user navigates to a web page, the browser will request and receive the HTML source code for that page. The browser can store the received HTML source code in memory so that it can be executed and the web page rendered for the user. In my opinion, these types of storage are distinct from “saving” information associated with a user’s browsing session, which implies that it will be retained even after the browser application is closed. Mr. Hochman has identified no evidence that Chrome Incognito Mode saves a user’s browsing history, cookies and site data, or information entered in forms so that it can be accessed after an Incognito Session ends. To the extent Mr. Hochman contends that storing information temporarily in memory constitutes “saving” that information, I disagree.

120. Based on my experience, review of documents, and testing results discussed above and in my opening report, Incognito Mode works as described to users by concealing users’ browsing activity from other people who may use the same device, and by ensuring that cookie

---

<sup>191</sup> GOOG-BRWN-00699213.

values generated during the Private Browsing Sessions cannot be used to provide a link to the user's browsing activity in Regular Mode.

## IX. OTHER REBUTTALS TO MR. HOCHMAN'S REPORT

### A. Mr. Hochman Exaggerates The Complexity Of Developer Tools

121. Mr. Hochman argues that Developer Tools<sup>192</sup> “are not designed for the use by typical Internet users, and they in any case do not provide information regarding exactly what private browsing information is collected by Google, what private browsing information is stored by Google, and/or how that private browsing information is exploited by Google.”<sup>193</sup> Mr. Hochman further claims that “[i]n my experience, those are not tools that any typical consumer would use or understand.”<sup>194</sup> Mr. Hochman fails to explain what kind of experience makes him come to this conclusion, and he offers no support as to who a “typical user” is and what technology experience they have.

122. While Developer Tools are designed for use by website developers, these tools are accessible to all users. For example, Developer Tools of Chrome and other browsers are accessible to a user with just two clicks. When a user right-clicks on the webpage in Chrome, a menu bar is displayed with a limited number of fields, one of which is “Inspect” as is illustrated in **Figure 8** below. After clicking on the “Inspect” field, the Chrome Developer Tools window will be opened. Alternatively, users can navigate to Developer Tools in Chrome by clicking on the three vertical

---

<sup>192</sup> I refer to Developer Tools as a collection of website inspection tools available in all popular browsers. See e.g., “Chrome DevTools,” *Chrome Developers*, Google, available at <https://perma.cc/9T24-5L9C>; “What are browser developer tools?” *MDN Web Docs*, available at <https://perma.cc/SL8Y-WSFP>.

<sup>193</sup> Hochman Report, ¶ 135.

<sup>194</sup> Hochman Report, ¶ 87.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

dots at the top right corner of the Chrome browser, expanding the “More tools” sub-menu, and clicking on “Developer Tools,” or by simply pressing “Ctrl + Shift + I,” as illustrated in **Figure 9**.

**Figure 8**  
**Accessing Developer Tools In Chrome Via “Inspect”**



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure 9**  
**Accessing Developer Tools In Chrome Via “Ctrl+Shift+I”**



123. Mr. Hochman also uses Developer Tools in his analysis of data that Chrome transmits to various domains in Incognito Mode, yet fails to explain why Developer Tools are adequate for that purpose but not others.<sup>195</sup> In my opening report, I used Chrome Developer Tools to illustrate the types of data, such as cookie values, that are stored and transmitted when browsing in Regular and Incognito Modes.<sup>196</sup> Observing that certain data are sent to Google when browsing a non-Google website does not require in-depth understanding of web technologies; a user can just type “google” in the respective search bar in the “Network tab” of Developer Tools as I illustrated in **Figure 10**. In fact, Chrome Developer Tools offers a “Help” webpage, accessible via a menu in

<sup>195</sup> Hochman Report, ¶ 87.

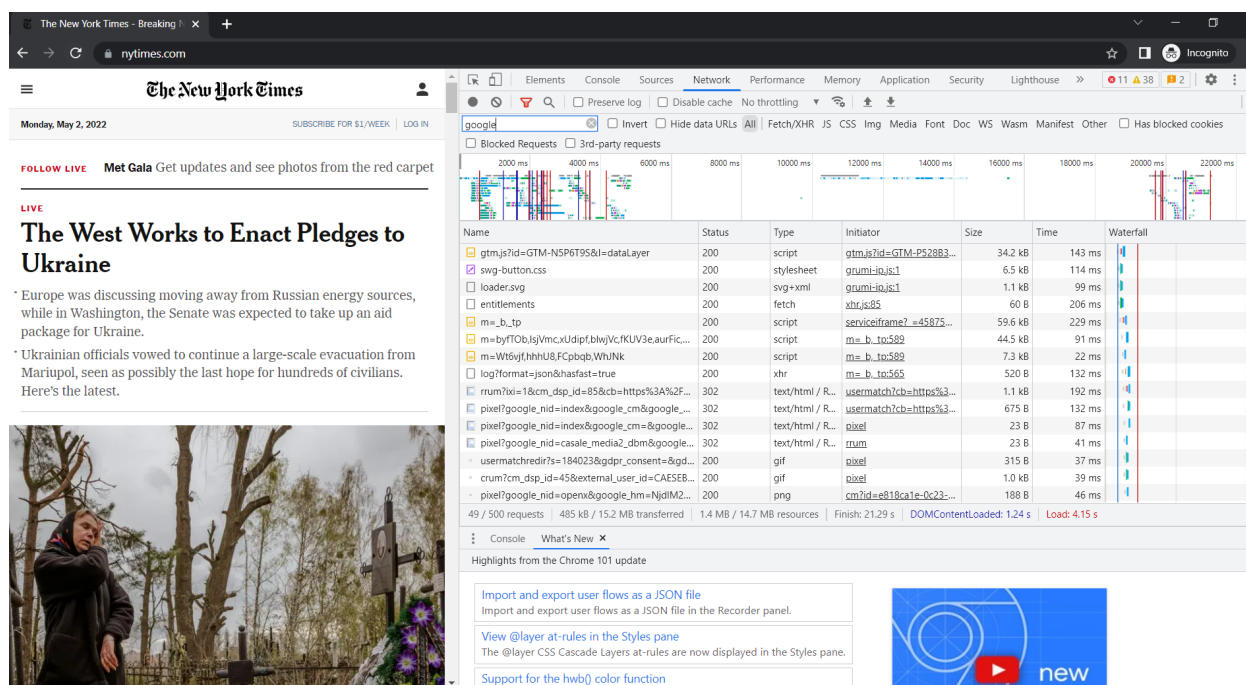
<sup>196</sup> See e.g., Zervas Affirmative Report, ¶¶ 63, 65-66.



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

the Developer Tools window, which explains the program to unfamiliar users.<sup>197</sup> Additionally, the “Inspect Network Activity” page includes a video explaining how to search for specific transmissions.<sup>198</sup>

**Figure 10**  
**Searching For Google-Related Transmission**



124. While many users may not be inclined to use Developer Tools, some users will. For example, users who want to review the technical details of a particular webpage or are interested in learning how websites and browsers work may use these tools to observe HTTP transmissions or view website source code. There are ample resources and support information available about Developer Tools and how to use them, such that holding a technical degree or having a deep

<sup>197</sup> “Chrome DevTools,” *Chrome Developers*, Google, available at <https://perma.cc/9T24-5L9C>.

<sup>198</sup> “Inspect network activity,” *Chrome Developers*, Google, February 8, 2019, available at <https://perma.cc/96JX-HTQF>.



technical background is not required for someone to use these tools. Therefore, I disagree with Mr. Hochman’s conclusions regarding the complexity of and information available to users of Developer Tools.

**B. Mr. Hochman’s Statements About Energy Saving And Performance Of Websites Related To Google’s Analytics And Advertising Services Are Flawed**

125. Mr. Hochman argues that “Google’s tracking beacons embedded in non-Google websites take up processing, storage, and power/battery resources to run on user devices; thereby increasing user’s energy and device costs.”<sup>199</sup> Mr. Hochman’s support for this conclusion is a single article, which does not even mention Google’s analytics and advertising services.<sup>200</sup>

126. This statement also assumes, without foundation, that in the absence of Google services, websites would not use other services to provide the same or similar functionality. As I explained in my opening report,<sup>201</sup> there are multiple alternatives that provide the same or similar functionality as the Google services at issue in this case, such as Hotjar,<sup>202</sup> Mixpanel,<sup>203</sup> Matomo,<sup>204</sup> Piwik PRO,<sup>205</sup> and Adobe Analytics.<sup>206</sup> Thus, I disagree with Mr. Hochman’s

---

<sup>199</sup> Hochman Report, ¶ 94.

<sup>200</sup> Pearce, Joshua, M., “Energy Conservation with Open Source Ad Blockers,” *MDPI*, Vol. 8, No. 2, 2020, available at <https://perma.cc/USH9-AQ8F>.

<sup>201</sup> Zervas Affirmative Report, ¶ 87.

<sup>202</sup> “Understand how users behave on your site, what they need, and how they feel, fast,” *Hotjar*, available at <https://perma.cc/PFP2-TD6F>.

<sup>203</sup> “Build Better Products,” *Mixpanel*, available at <https://perma.cc/7AV6-ZBHZ>.

<sup>204</sup> “Google Analytics alternative that protects your data and your customers’ privacy,” *Matomo*, available at <https://perma.cc/2FG3-BHM7>.

<sup>205</sup> “Analyze the customer journey across websites and apps,” *PIWIK PRO*, available at <https://perma.cc/7MRA-9CBF>.

<sup>206</sup> “Analytics Anywhere in the Customer Journey,” *Adobe Analytics*, *Adobe*, available at <https://perma.cc/6DYL-5AH4>.

assumption that browsers would somehow operate more efficiently if websites did not use Google's services.

127. Also, as confirmed by my testing that I present in my opening report, visiting a website typically triggers many other requests beyond the requests to the first-party website and Google. Therefore, Mr. Hochman wrongfully associates all these negative consequences with Google. As an illustrative example, when I visited Plaintiffs' attorneys' website *http://www.forthepeople.com/* in Incognito Mode, only 11 percent of the third-party transmissions were to Google-associated domains. This is lower than the number of transmissions to another third-party domain *wistia.com*, which provides video hosting services and accounts for 33 percent of the third-party transmissions.<sup>207,208</sup>

**C. Mr. Hochman's Assertion That Users Cannot Request Deletion Of Private Browsing Data Incorrectly Assumes That Google Can Identify Specific Users Associated With The Data**

128. Mr. Hochman argues that "[b]ased on my own experience as a Chrome user, and as confirmed by Halavati, Google does not give users the option to delete this data" that Google receives "when a user is in private browsing mode."<sup>209</sup> However, Mr. Hochman's opinion incorrectly assumes that Google can identify the specific users associated with browsing data from Private Browsing Sessions. But it is precisely because cookie values from Private Browsing Sessions in which the user does not sign into a Google account cannot be used as a link to the user or her device after the session is closed that the users are not able to delete that activity. As

---

<sup>207</sup> "The Video Host with the Most," *Wistia*, available at <https://perma.cc/BR2B-UZ9W>.

<sup>208</sup> I listed all domains and the corresponding number of observed transmissions in my backup materials.

<sup>209</sup> Hochman Report, ¶ 103.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Mr. Halavati explained, data from Private Browsing Sessions “are not connected to a user identity” and therefore Google cannot give users the option to delete this information “because it doesn’t know to which user they belong.”<sup>210</sup> Indeed, Mr. Hochman’s implicit assertion that Google should give users the ability to delete data generated while they were in Private Browsing Mode would *require* Google to associate that data with the users’ Google accounts (including their email addresses and other potentially identifying information), thereby *reversing* that privacy-enhancing feature of Incognito Mode.

Signed on the 7th day of June, 2022, at Brookline, MA.



---

Georgios Zervas

---

<sup>210</sup> Deposition of Ramin Halavati, January 18, 2022, p. 89:2-3.

# Georgios Zervas

Boston University  
Questrom School of Business  
595 Commonwealth Ave (Ofc. 605)  
Boston, MA 02215

Phone: (617) 358-3319 (office)  
Email: [zg@bu.edu](mailto:zg@bu.edu)  
Homepage: <http://people.bu.edu/zg/>  
Google Scholar: <https://scholar.google.com/citations?user=5L8vEA4AAAAJ>

*Last updated: Dec. 21, 2021*

## Employment & Affiliations

### Current

<b>Associate Professor of Marketing</b> Questrom School of Business, Boston University, Boston, MA	2019–to date
<b>Faculty Director, MS in Business Analytics</b> Questrom School of Business, Boston University, Boston, MA	2019–to-date
<b>Founding Member, Faculty of Computing &amp; Data Science</b> Boston University, Boston, MA	2019–to date
<b>Affiliated Faculty in Computer Science</b> Boston University, Boston, MA	2016–to date
<b>Visiting Researcher</b> Microsoft Research New England, Cambridge, MA	2013–to date

### Prior

<b>Assistant Professor of Marketing</b> Questrom School of Business, Boston University, Boston, MA	2013–2019
<b>Visiting Scholar</b> MIT Sloan, Cambridge, MA	Spring 2018
<b>Simons Postdoctoral Fellow</b> Yale University, New Haven, CT <i>Advisor:</i> Joan Feigenbaum	2011–2013
<b>Affiliate at the Center for Research &amp; Computation in Society</b> Harvard University, Cambridge, MA	2011–2013
<b>Research Scientist</b> CogoLabs Inc., Cambridge, MA, USA	2006–2012
<b>Cofounder</b> Perlfect Solutions, London, UK	2000–2005

## Education

- Ph.D. Computer Science** 2005–2011  
 Boston University, Boston, MA, USA.  
*Thesis:* Data-Driven Analysis of Electronic Commerce Systems.  
*Advisors:* John W. Byers (BU) & Michael Mitzenmacher (Harvard).
- M.A. Interactive Media** 1999–2000  
 London College of Communication, London, UK.  
*Thesis:* Automatic Website Generation Using Genetic Algorithms.  
*Advisor:* Alan Sekers.
- M.Sc. Computer Science** 1998–1999  
 Imperial College, London, UK.  
*Thesis:* Thesis: Advanced Clustering Algorithms.  
*Advisor:* Stefan Rüger.
- B.Eng. Computer Science** 1995–1998  
 Imperial College, London, UK.  
*Thesis:* Object Linking & Embedding for Linux.  
*Advisor:* Steffen van Bakel.

## Publications

### Journals

- Shrabastee Banerjee, Chris Dellarocas Chris, and Georgios Zervas  
**Interacting User-Generated Content Technologies: How Questions and Answers Affect Consumer Reviews.**  
*Journal of Marketing Research*, (2021);58(4): 742-761.
- Georgios Zervas, Davide Proserpio, and John W. Byers  
**A first look at online reputation on Airbnb, where every stay is above average**  
*Marketing Letters*, (2020): 1-16.
- Giana Eckhardt, Mark Houston, Baojun Jiang, Cait Lamberton, Aric Rindfleisch, and Georgios Zervas  
**Marketing in the Sharing Economy**  
*Journal of Marketing*, 83.5 (2019): 5-27.
- Giana Eckhardt, Mark Houston, Baojun Jiang, Cait Lamberton, Aric Rindfleisch, and Georgios Zervas  
**Marketing in the Sharing Economy**  
*Journal of Marketing*, 83.5 (2019): 5-27.
- Davide Proserpio, Wendy Xu, and Georgios Zervas  
**You Get What You Give: Theory and Evidence of Reciprocity in the Sharing Economy**  
*Quantitative Marketing and Economics*, 16(4), (2018): 371-407.
- Georgios Zervas, Davide Proserpio, and John W. Byers  
**The Rise of the Sharing Economy: Estimating the Impact of Airbnb on the Hotel Industry**  
*Journal of Marketing Research*, 54, no. 5 (2017): 687-705.  
 – Finalist for the 2018 Paul E. Green Award.

7. Davide Proserpio and Georgios Zervas  
**Online Reputation Management: Estimating the Impact of Management Responses on Consumer Reviews**  
*Marketing Science*, 36, no. 5 (2017): 645-665  
 – Finalist for the 2018 John D. C. Little Award.
8. Michael Luca, and Georgios Zervas  
**Fake It Till You Make It: Reputation, Competition, and Yelp Review Fraud**  
*Management Science*, 62, no. 12 (2016): 3412-3427

### Full Papers in Peer-reviewed Conferences with Proceedings

1. Ceren Budak, Sharad Goel, Justin M. Rao, and Georgios Zervas  
**Understanding Emerging Threats to Online Advertising**  
 In *Proceedings of the Sixteenth ACM Conference on Economics and Computation (EC '16)*. ACM, 2016.
2. John Byers, Michael Mitzenmacher, and Georgios Zervas  
**The Daily Deals Marketplace: Empirical Observations and Managerial Implications**  
 In *ACM SIGecom Exchanges*, Vol. 11, No. 2, December 2012, Pages 29–31.
3. Joan Feigenbaum, Michael Mitzenmacher, and Georgios Zervas  
**An Economic Analysis of User-Privacy Options in Ad-Supported Services**  
 In *Proceedings of the 8th Workshop on Internet & Network Economics*, WINE '12, pages 30–43. Springer Berlin Heidelberg, 2012.
4. John W. Byers, Michael Mitzenmacher, and Georgios Zervas  
**The Groupon Effect on Yelp Ratings: A Root Cause Analysis**  
 In *Proceedings of the 13th ACM Conference on Electronic Commerce*, EC '12, pages 248–265. Valencia, Spain, 2012. ACM.
5. John W. Byers, Michael Mitzenmacher, and Georgios Zervas  
**Daily Deals: Prediction, Social Diffusion, and Reputational Ramifications**  
 In *Proceedings of the 5th ACM international conference on Web Search and Data Mining*, WSDM '12, pages 543–552. Seattle, WA, USA, 2012. ACM.
6. John W. Byers, Brent Heeringa, Michael Mitzenmacher, and Georgios Zervas.  
**Heapable Sequences and Subsequences**  
 In *Proceedings of the Workshop on Analytic Algorithmics and Combinatorics*, ANALCO '11, pages 33–44, San Fransisco, CA, USA, 2011. ACM.
7. John W. Byers, Michael Mitzenmacher, and Georgios Zervas  
**Information asymmetries in pay-per-bid auctions**  
 In *Proceedings of the 11th ACM conference on Electronic Commerce*, EC '10, pages 1–12, New York, NY, USA, 2010. ACM.
8. John W. Byers, Michael Mitzenmacher, and Georgios Zervas  
**Adaptive Weighing Designs for Keyword Value Computation**  
 In *Proceedings of the third ACM international conference on Web search and data mining*, WSDM '10, pages 331–340, New York, NY, USA, 2010. ACM.
9. Nikolaos Laoutaris, Georgios Zervas, Azer Bestavros, and George Kollios  
**The Cache Inference Problem and its Application to Content and Request Routing**  
 In *Proceedings of the 26th Annual IEEE Conference on Computer Communications*, INFOCOM '07, pages 848–856, Anchorage, AK, USA, 2007. IEEE.

10. Georgios Zervas, and Stefan M. Rüger  
**The Curse of Dimensionality and Document Clustering**  
 In *IEEE Seminar, Searching for Information: Artificial Intelligence and Information Retrieval Approaches*, pages 19/1–19/3, Glasgow, UK, 1999.

### Abstracts in Peer-reviewed Conferences with Proceedings

1. Greg Lewis and Georgios Zervas  
**The Supply and Demand Effects of Review Platforms**  
 In *Proceedings of the 2019 ACM Conference on Economics and Computation (EC '19)*, pp. 197-197. ACM, 2019.
2. Shrabastee Banerjee, Chris Dellarocas, and Georgios Zervas  
**Interacting User Generated Content Technologies: How Q&As Affect Ratings & Reviews**  
 In *Proceedings of the 2017 ACM Conference on Economics and Computation (EC '17)*, pp. 539-539. ACM, 2017.
3. Georgios Zervas, Davide Proserpio, and John W. Byers  
**The Impact of the Sharing Economy on the Hotel Industry: Evidence from Airbnb's Entry Into the Texas Market**  
 In *Proceedings of the 2015 ACM Conference on Economics and Computation (EC '15)*, pp. 637-637. ACM, 2015.
4. Davide Proserpio and Georgios Zervas  
**Online Reputation Management: Estimating the Impact of Management Responses on Consumer Reviews**  
 In *Proceedings of the 2015 ACM Conference on Economics and Computation (EC '15)*, pp. 79-79. ACM, 2015.

### Invited Articles

1. Davide Proserpio and Georgios Zervas  
**Replying to Customer Reviews Results in Better Ratings**  
*Harvard Business Review*, Feb. 14, 2018.

### Working Papers

1. Greg Lewis, Bora Ozaltun, and Georgios Zervas  
**Maximum Likelihood Estimation of Differentiated Products Demand Systems**
2. Luis Armona, Greg Lewis, and Georgios Zervas  
**Learning Product Characteristics and Consumer Preferences from Search Data**
3. Stephan Seiler, Song Yao, Georgios Zervas  
**Causal Inference in Word-of-Mouth Research: Methods and Results**
4. Chiara Farronato and Georgios Zervas  
**Consumer Reviews and Regulation: Evidence from NY Restaurants**
5. Greg Lewis and Georgios Zervas  
**The Welfare Impact of Consumer Reviews: A Case Study of the Hotel Industry**
6. Greg Lewis and Georgios Zervas  
**Supply and Demand Responses to Consumer Review Platforms**

## Grants, Awards, & Honors

1. Marketing Science Institute (MSI) Young Scholars 2019
2. Dean's Research Scholar, Questrom School of Business 08/2018
3. Shahdadpuri Research Award, Questrom School of Business 10/2017
4. Hariri Institute Graduate Fellowship (\$25,000 award) 6/2015
5. Google Faculty Research Award (\$35,000 unrestricted gift, plus \$10,000 in Google Cloud credits) 2/2015
6. Hariri Institute Junior Faculty Fellow 2013–2015
7. Hariri Institute Research Grant Principal Investigator, with co-PI John W. Byers (\$26,500) 1/2013
8. Departmental Research Achievement Award, Computer Science Dept., Boston U. 2010–2011

## Student Advising

1. Hannah Catabia, PhD Student, Computer Science Dept., Co-advisor 2019–to date
2. Philip Zhao, PhD Student, Marketing Dept., Advisor 2018–to date
3. Shrabastee Banerjee, PhD Student, Marketing Dept., Advisor 2015–2021  
*Placement:* Tilburg University, Marketing
4. Davide Proserpio, PhD Student, Computer Science Dept., Co-advisor 2012–2015  
*Placement:* USC Marshall, Marketing

## Presentations and Invited Talks

### Learning Market Structure & Consumer Preferences from Search Data: An Application to Hotel Demand Estimation

#### Conferences:

- Marketing Science 2019, Rome, Italy 06/20/2019

### Consumer Reviews and Regulation: Evidence from NY Restaurants

#### Academia:

- Technische Universität Berlin, Germany 10/04/2021
- Universität zu Köln, Germany 07/31/2021
- Brandeis University, Waltham, MA 04/07/2021
- Yale School of Management, New Haven, CT 10/30/2020
- University of Miami, Miami, FL 10/23/2020
- UMass Amherst Isenberg School of Management, Amherst, MA 02/03/2018

#### Conferences:

- Marketing Science 2018, Philadelphia, PA 06/14/2018



Georgios Zervas, Associate Professor of Marketing, Questrom School of Business, Boston University

6

- BU Data Science Day, Boston University, Boston MA 01/26/2018
- Digital, Mobile Marketing, and Social Media Analytics Conference, NYU, New York, NY 09/12/2017
- Marketing Science, USC Marshall, Los Angeles, CA 06/10/2017
- Health Sector Data Blitz, Questrom School of Business, Boston, MA 03/11/2017
- Marketing Analytics and Big Data conference, Columbia University, New York, NY 16/09/2017

**The Welfare Impact of Consumer Reviews: A Case Study of the Hotel Industry**

## Academia:

- HEC, Paris, France 11/07/2019
- Duke Fuqua, Durham, North Carolina 05/01/2019
- Harvard Business School, Boston, MA 03/12/2019
- NYU Stern, New York, NY 02/14/2019
- Columbia GSB, New York, NY 10/16/2018
- USC Marshall, Los Angeles, CA 4/14/2017
- Stanford GSB, Palo Alto, CA 4/12/2017
- Michigan Ross, Ann Arbor, MI 4/10/2017
- University of Toronto Rotman, Toronto, ON 2/17/2017
- University of Chicago Booth, Chicago, IL 1/31/2017
- Wharton, Philadelphia, PA 1/25/2017
- MIT Economics Dept., Cambridge, MA 10/24/2016

## Conferences:

- QME 2016, Kellogg School of Management, Evanston, IL 09/01/2016
- SCECR 2016, Naxos, Greece 06/24/2016
- Greater China Conference on Mobile Big Data Marketing, Hong Kong 06/13/2016
- Marketing Science 2016, Shanghai, China 06/16/2016

**Online Reputation Management: Estimating the Impact of Management Responses on Consumer Reviews.**

## Academia:

- Harvard EconCS Seminar, Cambridge, MA 10/02/2015
- Hebrew University, Computer Science dept., Jerusalem, Israel 06/14/2015

**The Rise of the Sharing Economy: Estimating the Impact of Airbnb on the Hotel Industry**

## Conferences:

- Open & User Innovation Conference 2015, Harvard Business School, Boston MA 08/03/2016
- CODE@MIT, Cambridge MA 10/16/2015
- Marketing Science 2015, Baltimore 05/20/2015
- NYU 2015 Conference on Digital Big Data, Smart Life, Mobile Marketing Analytics 23/10/2015

## Academia:

- Simon Business School, University of Rochester 2/29/2016

## Industry:

- Microsoft Research New England 11/18/2015

Georgios Zervas, Associate Professor of Marketing, Questrom School of Business, Boston University

7

Government:

- Cambridge City Council, Cambridge, MA 7/19/2016

**Understanding Emerging Threats to Online Advertising**

Academia:

- Goizueta Business School, Emory University 02/27/2015
- MSR/Harvard Game Theory Seminar 12/17/2014
- Questrom School of Business, MPPL Seminar 04/17/2015

Industry:

- Betaworks, NYC 07/23/2015

**Fake It Till You Make It: Reputation, Competition, and Yelp Review Fraud**

Conferences:

- Marketing Science 2014, Emory University, Atlanta 06/13/2014
- WIN 2013: The 5th Workshop on Information in Networks 10/04/2013
- DIMACS Workshop on Economic Aspects of Information Sharing 02/08/2013

Industry:

- Google, Palo Alto, CA 02/12/2013

**The Groupon Effect on Yelp Ratings: A Root Cause Analysis**

Conferences:

- Marketing Science 2013, Istanbul, Turkey 07/13/2013
- SCECR 2012, Montreal, Canada 06/29/2012
- ACM EC 2012, Valencia, Spain 06/05/2012
- Yale Customer Insights Conference, New Haven, CT 03/15/2013
- CAOSS 2012: Workshop on Computational and Online Social Science, New York, NY 10/12/2012

Academia:

- Wellesley University, Computer Science Dept 02/27/2012
- Northeastern University, Computer Science Dept 03/28/2012
- Harvard University, School of Eng. & Appl. Sci., Joint EconCS/Theory Seminar 04/16/2012
- Berkeley University, Computer Science Dept 04/10/2012

Industry:

- Microsoft Research New York 02/27/2013
- Google, Palo Alto, CA 04/09/2012
- Yelp, San Francisco, CA 04/11/2012

**Daily Deals: Prediction, Social Diffusion, and Reputational Ramifications**

Conferences:

- New York Computer Science and Economics Day (*Poster session.*) 09/16/2011
- Cambridge Area Economics and Computation Day (*Poster session.*) 11/18/2011
- ACM WSDM 2012 02/11/2012

**Academia:**

- Harvard University, School of Eng. & Appl. Sci., Joint EconCS/Theory Seminar 10/20/2011
- Boston University, Mathematics Dept., Statistics and Probability Seminar 11/17/2011
- Columbia University, Computer Science Dept., Seminar 12/08/2011

**Industry:**

- IBM Research, Hawthorne, NY, Seminar 12/07/2011
- Microsoft Research New England, Economics Research Working Group 10/14/2011

**Information Asymmetries in Pay-Per-Bid Auctions: How Swoopo Makes Bank****Conferences:**

- ACM EC 2010 06/09/2010

**Academia:**

- Boston University, Computer Science Dept., Theory Seminar 03/19/2010
- Harvard University, School of Eng. & Appl. Sci., Joint EconCS/Theory Seminar 03/29/2010
- Northeastern University, Coll. of Comp. & Inf. Sci., Graduate Student Seminar 04/03/2010
- Williams College, Computer Science Dept., Invited Colloquium 10/22/2010

**Adaptive Weighing Designs for Keyword Value Computation****Conferences:**

- ACM WSDM 2010 02/06/2010

**Academia:**

- Boston University, Computer Science Dept., Networking Reading Group 02/08/2010
- Boston University, Computer Science Dept., CS565 Data Mining, Guest Lecture 03/23/2010

**Teaching**

1. BA810: Supervised Machine Learning (44 students) Fall 2019
2. BA810: Supervised Machine Learning (42 students) Fall 2019
3. MK476: Machine Learning for Business Analytics (26 students) Spring 2019
4. MK824: Machine Learning for Business Analytics (44 students) Spring 2019
5. MK824: Machine Learning for Business Analytics (40 students) Spring 2018
6. MK824: Machine Learning for Business Analytics (43 students) Spring 2017
7. MK323: Marketing Management (49 students) Spring 2017
8. MK323: Marketing Management (48 students) Fall 2015
9. MK323: Marketing Management (50 students) Fall 2015
10. MK323: Marketing Management (47 students) Fall 2014
11. MK323: Marketing Management (47 students) Fall 2014
12. MK323: Marketing Management (49 students) Fall 2013
13. MK323: Marketing Management (50 students) Fall 2013

## Course Development

**MK476**, **MK842**, and **BA810** are courses that I developed that introduce undergraduate, MBA, and MSBA students to machine learning methods with applications in business analytics.

## Service

**Editorial Review Board** 2020–to-date  
Marketing Science

**Steering Committee Member** 2019–to-date  
Rafik B. Hariri Institute for Computing, Boston University

**Editorial Review Board** 2019–to-date  
Journal of Marketing

**Editorial Review Board** 2019–to-date  
Journal of Marketing Research

**Associate Editor** 2019–to date  
ACM Transactions on Economics and Computation

**Program committees:** EC 2021 (Program Committee), EC 2020 (Senior Program Committee), WebConf 2020, EC 2019 (Senior Program Committee), EC 2018 (Senior Program Committee), EC 2018, WWW 2018, ICIS 2018, EC 2017 (Senior Program Committee), EC 2016 (Senior Program Committee), WWW 2016 (Senior Program Committee), ICIS 2016, SCECR 2016, EC 2015, WSDM 2015, WWW 2015, AMMA 2015, COBE 2015, EC 2014, WSDM 2014, WWW 2014, ICWSM 2014, WWW 2013, WSDM 2013, EC 2012.

**Ad-hoc reviewer:** Management Science, Marketing Science, Journal of Marketing Research, Information Systems Research, Games and Economic Behavior, Review of Industrial Organization, Operations Letters, Management Information Systems Quarterly, Journal of Public Economics, Manufacturing & Service Operations Management.

## Media coverage

1. [Some Smiling Faces in Online Customer Testimonials Are Stock Photos](#) 05/16/2019  
The Wall Street Journal
2. [Why ranting on Yelp is the wrong way to complain about awful service](#) 04/03/2018  
The Boston Globe
3. [Does a 'Sharing Economy' Foster Better Behavior?](#) 03/27/2018  
PC Magazine
4. [For Hotels, Online Reviews Really Matter to the Bottom Line](#) 11/18/2016  
The Wall Street Journal
5. [Don't Necessarily Judge Your Next E-Book By Its Online Review](#) 10/26/2015  
NPR All Things Considered
6. [Five-star fakes](#) 10/24/2015  
The Economist

Georgios Zervas, Associate Professor of Marketing, Questrom School of Business, Boston University

10

7. [Ratings Now Cut Both Ways, So Don't Sass Your Uber Driver](#) 01/30/2015  
The New York Times
8. [Airbnb, Uber, Lyft: de l'économie collaborative au business du partage](#) 08/16/2014  
Le nouvel Observateur
9. [Airbnb versus hotels: Room for all, for now](#) 04/26/2014  
The Economist
10. [Keeping crowdsourcing honest: can we trust the reviews?](#) 02/18/2014  
BBC News
11. [Why It's So Hard to Figure Out the Sharing Economy's Winners and Losers](#) 02/10/2014  
The Atlantic Cities
12. [Sharing Is Caring, Unless It Costs You Your Job](#) 02/05/2014  
The New York Times Bits Blog
13. [Yelp Reviews: Can You Trust Them?](#) 11/04/2013  
BU Today
14. [Fake reviews on Yelp?! Don't worry, we've got your back](#) 09/27/2013  
Yelp Official Blog
15. [Yelp deems 20% of user reviews 'suspicious'](#) 09/24/2013  
Marketwatch, The Wall Street Journal
16. [Yelp admits a quarter of submitted reviews could be fake](#) 09/13/2013  
BBC News
17. [Underdog Businesses Are More Likely to Post Fake Yelp Reviews](#) 08/30/2013  
Harvard Business Review Blog Network
18. [How Good Groupon Leads to Bad Yelp](#) 03/11/2013  
The Freaknomics Blog
19. [For Some Businesses, Daily Deals Have A Dark Side](#) 07/06/2012  
NPR Morning Edition
20. [Using Groupon Deals? Your Yelp Rating May Suffer](#) 04/11/2012  
The Huffington Post
21. [Help for Yelp](#) 11/09/2011  
BU Today
22. [Groupon IPO: An Internet star falls to Earth](#) 10/23/2011  
Christian Science Monitor
23. [Is Groupon Bad For Business?](#) 10/18/2011  
WBUR
24. [Groupon: Bad for Business?](#) 10/05/2011  
BU Today
25. [Groupon's Morning After Problem](#) 10/04/2011  
Time Magazine

*Georgios Zervas, Associate Professor of Marketing, Questrom School of Business, Boston University*

11

26. [Coupon Sites Are a Great Deal, but Not Always to Merchants](#) 10/02/2011  
The New York Times
27. [Groupon Deals May Hurt Your Yelp Ratings](#) 09/12/2011  
The Atlantic
28. [Study: Daily Deals Hurt Businesses' Reputations](#) 07/06/2011  
The Wall Street Journal, "In Charge" blog
29. [Groupon's Hidden Influence on Reputation](#) 09/12/2011  
The MIT Technology Review

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**APPENDIX B**

**LIST OF PRIOR EXPERT TESTIMONY FOR DR. GEORGIOS ZERVAS**

**Calhoun et al. v. Google LLC, U.S. District Court for the Northern District of California –  
San Jose Division, Case No. 5:20-cv-05146**

Expert Report (December 2021) and Deposition Testimony (January 2022).

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

## **Appendix C**

### **Materials Considered**

#### **Legal Documents**

Deposition of Justin Schuh, January 6, 2022.

Deposition of Michael Kleber, March 18, 2022.

Deposition of Ramin Halavati, January 18, 2022.

Deposition of Rory McClelland, February 18, 2022.

Expert Report of Dr. Georgios Zervas, April 15, 2022.

Expert Report of Jonathan E. Hochman, April 15, 2022.

Third Amended Class Action Complaint, Chasom Brown, et al., v. Google LLC, United States District Court Northern District of California, February 3, 2022.

#### **Bates Stamped Document**

GOOG-BRWN-00699213.

#### **Academic Literature**

Ahmad, Nadim, and Paul Schreyer, “Measuring GDP in a Digitalized Economy,” *OECD Statistics Working Papers*, No. 2016/07, 2016, available at <https://perma.cc/GNV6-GHRX>.

Bekh, Alona, “Advertising-based Revenue Model in Digital Media Market,” *Ekonomski vjesnik/Econviews - Review of Contemporary Business, Entrepreneurship and Economic Issues*, Vol. 33, No. 2, 2020, available at <https://perma.cc/W7QP-YTPM>.

Benzell, Seth G., Guillermo Lagarda, and Marshall Van Alstyne, “The Impact of APIs on Firm Performance,” *Boston University Questrom School of Business Research Paper*, available at <https://perma.cc/5FRY-WTSF>.

Berman, Ron, and Ayelet Israeli, “The Value of Descriptive Analytics: Evidence from Online Retailers,” *Harvard Business School*, Working Paper 21-067, 2021, available at <https://perma.cc/B7JY-V3UX>.

Brynjolfsson, Erik and Joo Hee Oh, “The Attention Economy: Measuring the Value of Free Digital Services on the Internet,” *Thirty Third International Conference on Information Systems, Orlando 2012*, 2012, available at <https://perma.cc/E2TZ-A6J9>.

Garett, Renee et al., “A Literature Review: Website Design and User Engagement,” *Online journal of communication and media technologies*, Vol. 6, No. 3, 2016, available at <https://perma.cc/PPC7-PWCM>.

Greenwood, Jeremy et al., “‘You Will’: A Macroeconomic Analysis of Digital Advertising,” *Economics of Digital Services @ Penn*, 2021, available at <https://perma.cc/ZX8P-9LC2>.



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Klym, Natalie and David Clark, “The Future of the Ad-Supported Internet Ecosystem,” *MIT Internet Policy Research Initiative*, 2019, available at <https://perma.cc/S6LC-KHPJ>.

Nakamura, Leonard, Jon Samuels, and Rachel Soloveichik, “Valuing ‘Free’ Media in GDP: An Experiment Approach,” *Federal Reserve Board of Philadelphia Working Paper*, No. 16-24, 2016, available at <https://perma.cc/4HMJ-7D3R>.

Pearce, Joshua, M., “Energy Conservation with Open Source Ad Blockers,” *MDPI*, Vol. 8, No. 2, 2020, available at <https://perma.cc/USH9-AQ8F>.

Schneier, Bruce, “Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,” W.W. Norton & Company, 2015.

Tidal, Junior R., “Using Web Analytics for Mobile Interface Development,” *New York City College of Technology*, 2013, available at <https://perma.cc/Z6Z8-U5MW>.

### **Publicly Available Sources**

“About enhanced conversions,” *Google Ads Help*, Google, available at <https://perma.cc/6UH8-9Q7X>.

“About publisher provided identifiers,” *Ad Manager Help*, Google, available at <https://perma.cc/P6WG-YX4S>.

“About Us: Helping your business leverage the Internet,” *Hochman Consultants*, available at <https://perma.cc/86E7-A39K>.

“Ad-Supported Internet Brings over \$1 Trillion to the U.S. Economy, Representing 6 Percent of Country's Total GDP, According to IAB Study Led by Harvard Business School Professor,” *Interactive Advertising Bureau*, March 15, 2017, available at <https://perma.cc/G9BS-85MJ>.

“Ad-Supported vs Subscription: Which is Better,” *Aniview*, December 11, 2021, available at <https://perma.cc/7NN2-XFEY>.

“Analytics Anywhere in the Customer Journey,” *Adobe Analytics*, Adobe, available at <https://perma.cc/6DYL-5AH4>.

“Analyze the customer journey across websites and apps,” *PIWIK PRO*, available at <https://perma.cc/7MRA-9CBF>.

“Apple Privacy Policy,” *Apple Privacy*, Apple, October 27, 2021, available at <https://perma.cc/839B-PPM5>.

“Build Better Products,” *Mixpanel*, available at <https://perma.cc/7AV6-ZBHZ>.

“BuzzFeed’s Privacy Policy and Cookie Policy,” *BuzzFeed*, October 8, 2021, available at <https://perma.cc/4WBC-XSC9>.

“Choose a Plan,” *Peacock*, available at <https://perma.cc/MLK5-GX59>.

“Chrome DevTools,” *Chrome Developers*, Google, available at <https://perma.cc/9T24-5L9C>.

“Cookie Notice,” *Reddit*, September 15, 2020, available at <https://perma.cc/M3WH-HDL9>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

“Cookie Policy,” *Indeed, Inc.*, November 1, 2021, available at <https://perma.cc/C6JR-WU5N>.

“Cookie Policy,” *Gannett*, October 5, 2020, available at <https://perma.cc/TRQ5-GSPU>.

“Cookie Policy,” *Grammarly*, December 30, 2019, available at <https://perma.cc/V5MQ-G8B9>.

“Cookie Policy,” *LinkedIn*, June 3, 2022, available at <https://perma.cc/K9RY-V8AE>.

“Cookie Policy,” *The New York Times*, September 17, 2021, available at <https://perma.cc/LN7U-H4Q3>.

“Cookies Policy,” *Insider Inc.*, September 4, 2019, available at <https://perma.cc/MH9H-5V3Z>.

“Cookies, web beacons, and similar technology (“Cookie Notice”),” *eBay Customer Service, eBay*, available at <https://perma.cc/5FMF-UC3J>.

“cp command in Linux with examples,” *GeeksforGeeks*, February 19, 2021, available at <https://perma.cc/2TV6-H3DY>.

“Definition of User Agent,” *W3C*, June 16, 2011, available at <https://perma.cc/5FCX-K45N>.

“Disable Google Analytics measurement,” *Google Analytics, Google*, available at <https://perma.cc/FXP9-3CGT>.

“Encyclopaedia Britannica, Inc. Privacy Notice,” *Encyclopedia Britannica*, November 10, 2021, available at <https://perma.cc/57Z7-EHZ5>.

“Google Analytics alternative that protects your data and your customers’ privacy,” *Matomo*, available at <https://perma.cc/2FG3-BHM7>.

“Google Analytics Blocker,” *Firefox Browser Add-Ons*, available at <https://perma.cc/L3RX-X2A6>.

“Google Chrome Privacy Notice,” *Google*, September 23, 2021, available at <https://perma.cc/SX4Q-3YU4>.

“Google Chrome,” *The Keyword, Google*, available at <https://perma.cc/5QFA-CBFC>.

“Google Privacy Policy,” *Google Privacy & Terms, Google*, available at <https://perma.cc/LYU9-8XTC>.

“Google Publisher Policies: Privacy-related policies: Privacy disclosures,” *Google Ad Manager Help, Google*, available at <https://perma.cc/G2FU-Z7PK>.

“Hearst.com Privacy Notice,” *Hearst Communications*, December 30, 2019, available at <https://perma.cc/6SKE-3CK7>.

“How Chrome Incognito keeps your browsing private,” *Google Chrome Help, Google*, available at <https://perma.cc/2YZX-VG2U>.

“HTML <script> Tag,” *W3Schools*, available at <https://perma.cc/KH7P-MY7D>.

“HTTP headers | User-Agent,” *GeeksforGeeks*, October 11, 2019, available at <https://perma.cc/QAA8-S428>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

“Indeed’s Full Privacy Policy,” *Indeed Inc.*, May 27, 2022, available at <https://perma.cc/HBC7-YGSK>.

“Inspect network activity,” *Chrome Developers, Google*, February 8, 2019, available at <https://perma.cc/96JX-HTQF>.

“Kohl’s Department Stores, Inc. — About Our Ads,” *Kohl’s Department Stores, Inc.*, August 12, 2016, available at <https://perma.cc/AU59-FHTK>.

“KOHL’S PRIVACY POLICY - YOUR PRIVACY RIGHTS,” *Kohl’s Department Stores, Inc.*, April 13, 2022, available at <https://perma.cc/TUB7-WLPN>.

“Limited Ads,” *Google Ad Manager Help, Google*, available at <https://perma.cc/MT25-D2C3>.

“Limits of User-ID view & Cross Device reports,” *Analytics Help, Google*, available at <https://perma.cc/BAM5-AYUB>.

“Manage user privacy,” *Google Analytics, Google*, available at <https://perma.cc/PVW7-EBB2>.

“Measurement Protocol, SKD, and User ID Feature Policy,” *Google Analytics, Google*, available at <https://perma.cc/88W2-LDYD>.

“Policy on Cookies, Web Beacons, Pixels, and Similar Technologies,” *AccuWeather*, May 25, 2019, available at <https://perma.cc/EJ4S-M8EJ>.

“Privacy & Cookies Policy (the “Policy”),” *Associated Newspapers Ltd*, March 10, 2022, available at <https://perma.cc/R3WW-44FY>.

“Privacy & Cookies Policy,” *Chaturbate*, May 25, 2022, available at <https://perma.cc/WN3X-ZS9J>.

“Privacy Notice,” *Hearst Television Inc.*, June 2020, available at <https://perma.cc/84RP-6H7H>.

“Privacy Notice,” *Momentive*, August 16, 2021, available at <https://perma.cc/J5FX-6XPL>.

“Privacy Notice,” *New York Post*, January 20, 2022, available at <https://perma.cc/NG69-7CFQ>.

“Privacy Notice,” *Realtor.com*, December 7, 2021, available at <https://perma.cc/QQ66-TJJA>.

“Privacy Policy and Cookie Statement,” *Condé Nast*, February 18, 2022, available at <https://perma.cc/QN2J-686R>.

“Privacy Policy,” *AccuWeather*, August 21, 2020, available at <https://perma.cc/4NT5-WCHW>.

“Privacy Policy,” *Change.org*, March 25, 2022, available at <https://perma.cc/G2HG-5AEV>.

“Privacy Policy,” *Chess.com*, April 21, 2022, available at <https://perma.cc/J4R2-JDBM>.

“Privacy Policy,” *Fandom, Inc.*, May 24, 2022, available at <https://perma.cc/8PRV-RMMT>.

“Privacy Policy,” *Fox News Network, LLC*, November 10, 2021, available at <https://perma.cc/5C3E-C62W>.

“Privacy Policy,” *LinkedIn*, August 11, 2020, available at <https://perma.cc/2TT8-37Q2>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

“Privacy Policy,” *Nexstar Media Group Inc.*, December 31, 2019, available at <https://perma.cc/8T7E-MAKP>.

“Privacy Policy,” *Paramount*, March 10, 2021, available at <https://perma.cc/7Y87-LL46>.

“Privacy Policy,” *Pornhub*, April 14, 2022, available at <https://perma.cc/2VZY-KJ6A>.

“Privacy Policy,” *Privy*, December 20, 2019, available at <https://perma.cc/A8HS-5M6E>.

“Privacy Policy,” *Publishers Clearing House*, May 21, 2021, available at <https://perma.cc/RU2Q-5JVK>.

“Privacy Policy,” *The New York Times*, February 3, 2022, available at <https://perma.cc/3FUW-2XYP>.

“Privacy Policy,” *The Washington Post*, October 5, 2021, available at <https://perma.cc/5WVW-YRQV>.

“Privacy Policy,” *The Weather Company*, available at <https://perma.cc/H6XL-5KM3>.

“Privacy Policy,” *Worldometers.info*, available at <https://perma.cc/TP5H-BSNH>.

“Privacy Policy,” *Zynga*, May 31, 2022, available at <https://perma.cc/EHW7-G4J6>.

“Private Browsing - Use Firefox without saving history,” *Mozilla Support*, available at <https://perma.cc/X9NG-QCB8>.

“Protecting your privacy online,” *The Privacy Sandbox, Google*, available at <https://perma.cc/C2TM-927B>.

“Quizlet Ad and Cookie Policy,” *Quizlet*, January 1, 2020, available at <https://perma.cc/UQ3J-8QX4>.

“Quizlet Privacy Policy,” *Quizlet*, August 17, 2021, available at <https://perma.cc/Z7ZY-YKFS>.

“Roblox Privacy and Cookie Policy,” *Roblox*, June 3, 2022, available at <https://perma.cc/2EXQ-5Q3Q>.

“Set up enhanced conversions for web manually with Google Tag Manager”, *Google Ads Help, Google*, available at <https://perma.cc/CR99-8WUE>.

“Share of digital in newspaper advertising revenue in the United States from 2011 to 2020,” *Statista*, available at <https://perma.cc/P88K-7CQK>.

“Statement on Cookies and Tracking Technologies,” *PayPal*, May 25, 2018, available at <https://perma.cc/2PZR-8P87>.

“Strategies for carrying out testing,” *MDN Web Docs*, available at <https://perma.cc/F5G6-KN2C>.

“Target Privacy Policy,” *Target*, July 1, 2021, available at <https://perma.cc/38A3-CJZ7>.

“The Internet Marketing Process,” *Hochman Consultants*, available at <https://perma.cc/Y354-MANZ>.

“The New York Times Company Reports First-Quarter 2022 Results,” *The New York Times Company*, May 4, 2022, available at <https://perma.cc/QR4R-EHP6>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

“The Video Host with the Most,” *Wistia*, available at <https://perma.cc/BR2B-UZ9W>.

“Three Ways APIs Are Keeping Small Businesses Digitally Competitive,” *Small Business Trends*, February 10, 2022, available at <https://perma.cc/6W7V-ZR5N>.

“TownNews Privacy Statement,” *TownNews*, June 30, 2020, available at <https://perma.cc/S2NP-6YRS>.

“Understand how users behave on your site, what they need, and how they feel, fast,” *Hotjar*, available at <https://perma.cc/PFP2-TD6F>.

“User-ID limits,” *Analytics Help, Google*, available at <https://perma.cc/V6BT-9A8X>.

“VDO.AI Terms and Conditions,” *VDO.AI*, available at <https://perma.cc/M6RL-2ZKH>.

“W3C TAG Observations on Private Browsing Modes,” *World Wide Web Consortium*, April 9, 2020, available at <https://perma.cc/8SLY-NZ66>.

“WarnerMedia News and Sports Privacy Policy,” *WarnerMedia*, April 8, 2022, available at <https://perma.cc/U3PC-YX2X>.

“WebMD Cookie Policy,” *WebMD*, April 28, 2022, available at <https://perma.cc/ED44-6Z33>.

“What are browser developer tools?” *MDN Web Docs*, available at <https://perma.cc/SL8Y-WSFP>.

“Without our members, there is no LinkedIn,” *LinkedIn*, available at <https://perma.cc/3W7E-HA7Y>.

“Yummly Privacy Notice & Your Privacy,” *Yummly*, December 2021, available at <https://perma.cc/L2H5-MHSD>.

Benton, Joshua, “Your favorite way to get around The New York Times paywall might be about to go away,” *NiemanLab*, February 28, 2019, available at <https://perma.cc/F5ED-BV3H>.

Bradshaw, Kyle, “Google wants to make it harder for sites to detect that you’re using Chrome’s Incognito Mode,” *9to5Google*, February 15, 2019, available at <https://perma.cc/QSX5-J6RV>.

Deighton, John, A., and Leora D. Kornfeld, “Economic Value of the Advertising-Supported Internet Ecosystem,” *Interactive Advertising Bureau*, September 2012, available at <https://perma.cc/2SS5-CGJK>.

Orgera, Scott, “How to Disable JavaScript in Firefox,” *Lifewire*, December 2, 2020, available at <https://perma.cc/5GLL-U868>.

Sabanovic, Edin, “How to Use Google Analytics to Improve Your Web Design Projects,” *Shopify Partners, Shopify*, June 13, 2017, available at <https://perma.cc/QG8Y-JYD8>.

Zacks Equity Research, “Subscription Revenues a Key Driver for NY Times (NYT) in 2022,” *Yahoo*, December 21, 2021, available at <https://perma.cc/BGY8-EHW7>.

## Appendix D

### Privacy Policy Screenshots

I reviewed the top 25 websites for Google Analytics and Google Ad Manager referred to by Mr. Hochman.<sup>1</sup> Except for few instances where a website was not accessible or the privacy policy was not applicable,<sup>2</sup> all websites contained a privacy notice page which was accessible in Private Browsing Mode in Chrome, Edge, and Safari, as illustrated in Figures below for all the examples I discuss in **Section IV.A** of my report.<sup>3,4</sup>

---

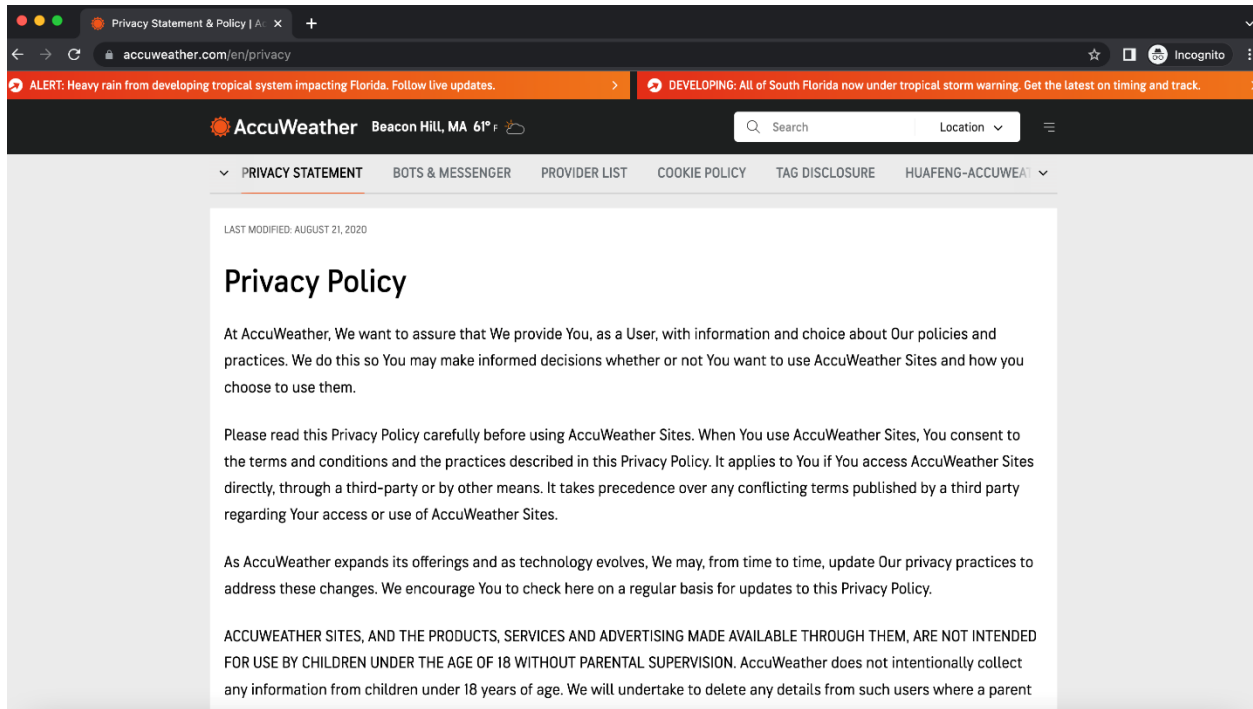
<sup>1</sup> See e.g., Hochman Report, ¶ 134.

<sup>2</sup> For example, <https://howto.gov/> was not accessible; <https://wikia.com/> redirected to <https://fandom.com/> which contained privacy notices; <https://condenastinternational.com/> redirected to <https://condenast.com/> which contained privacy notices; certain websites included in the list are duplicated to another website in the list. For examples, <https://mobile.nytimes.com/> is a duplicate to <https://nytimes.com/>. Both have a common privacy notices webpage <https://www.nytimes.com/privacy/privacy-policy/>.

<sup>3</sup> I use macOS since the current version of Safari cannot be used on Windows, but the current versions of Chrome, Edge, and Safari can be used on macOS.

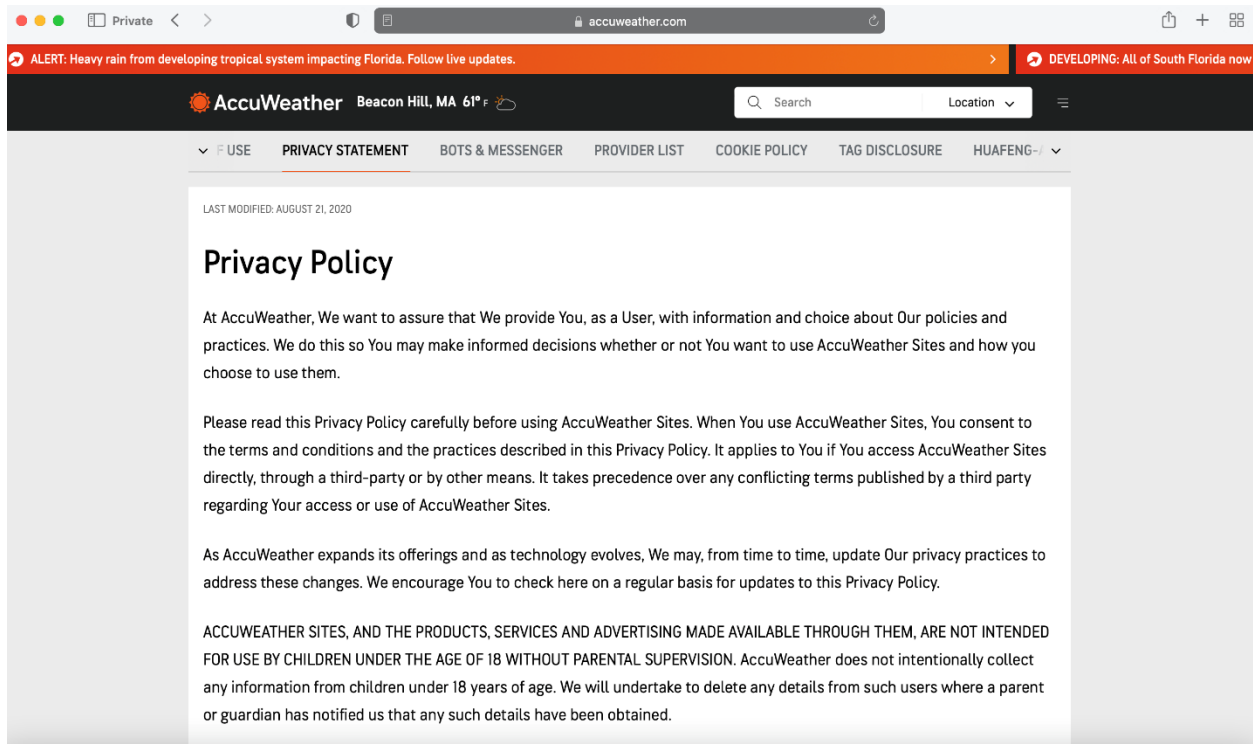
<sup>4</sup> The full review of all accessible websites referred to by Mr. Hochman is included in my backup production.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.1.1****AccuWeather.com - Chrome**

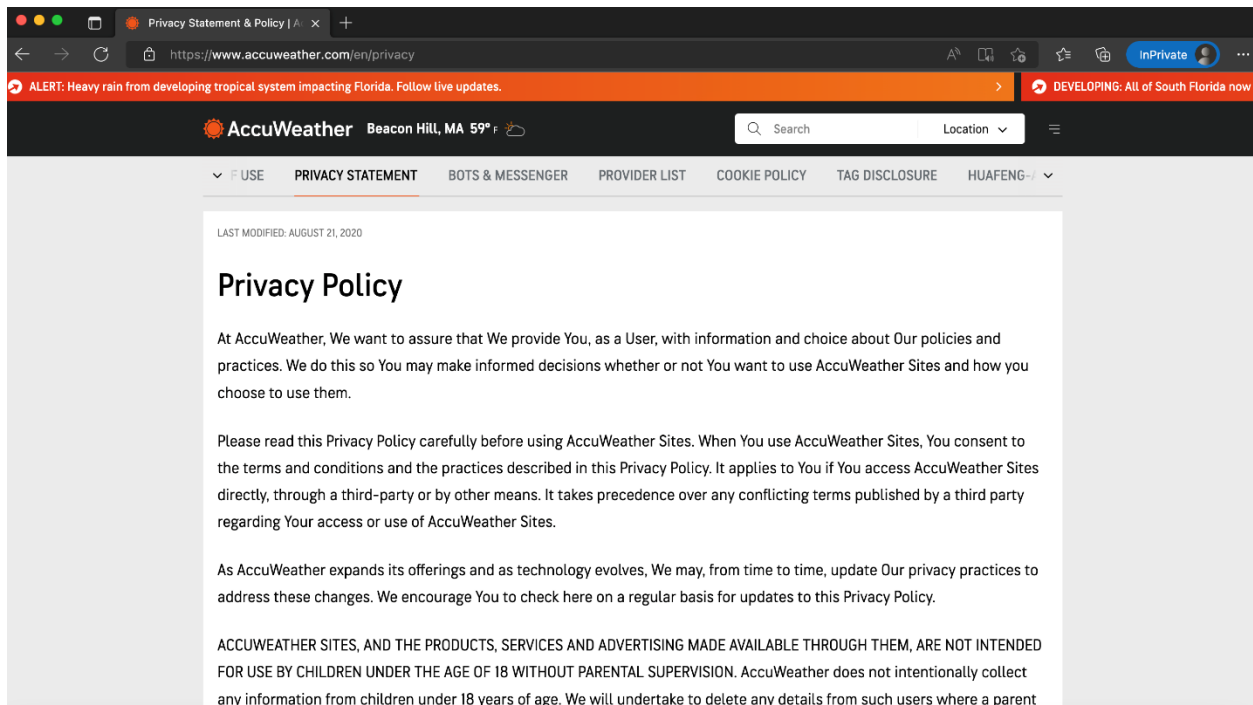


CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.1.2****AccuWeather.com - Safari**



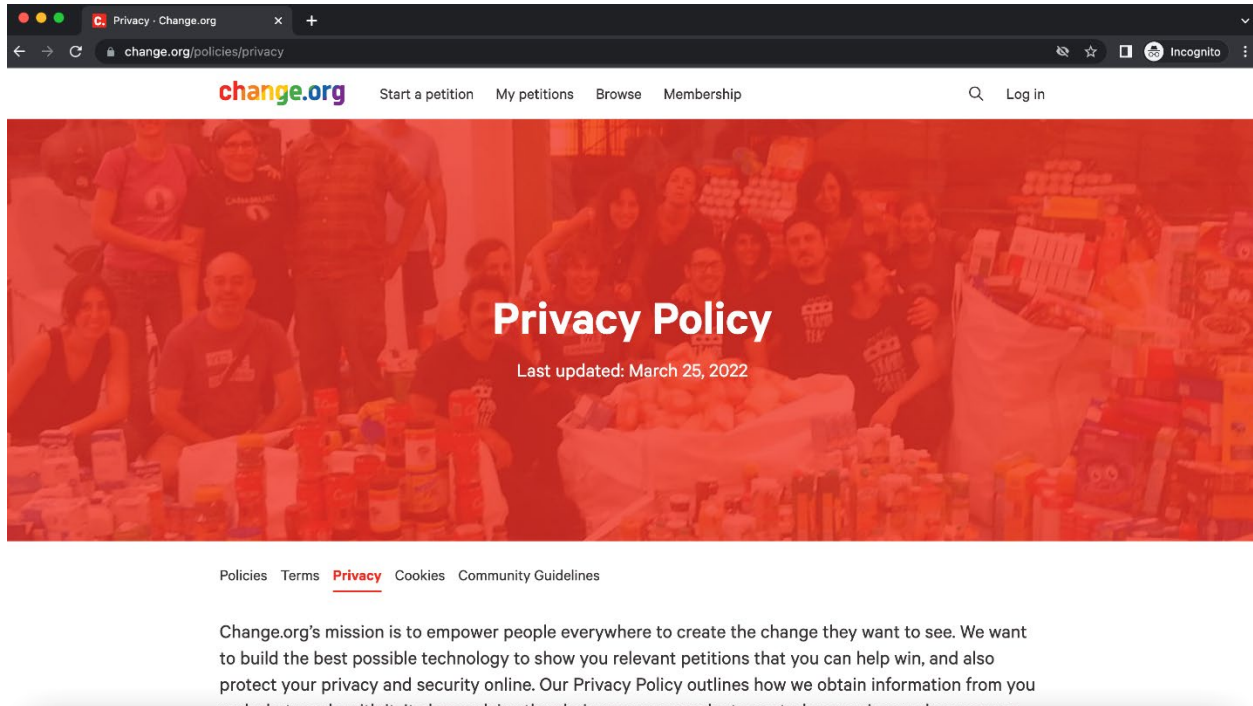
CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.1.3****AccuWeather.com - Edge**

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.2.1**

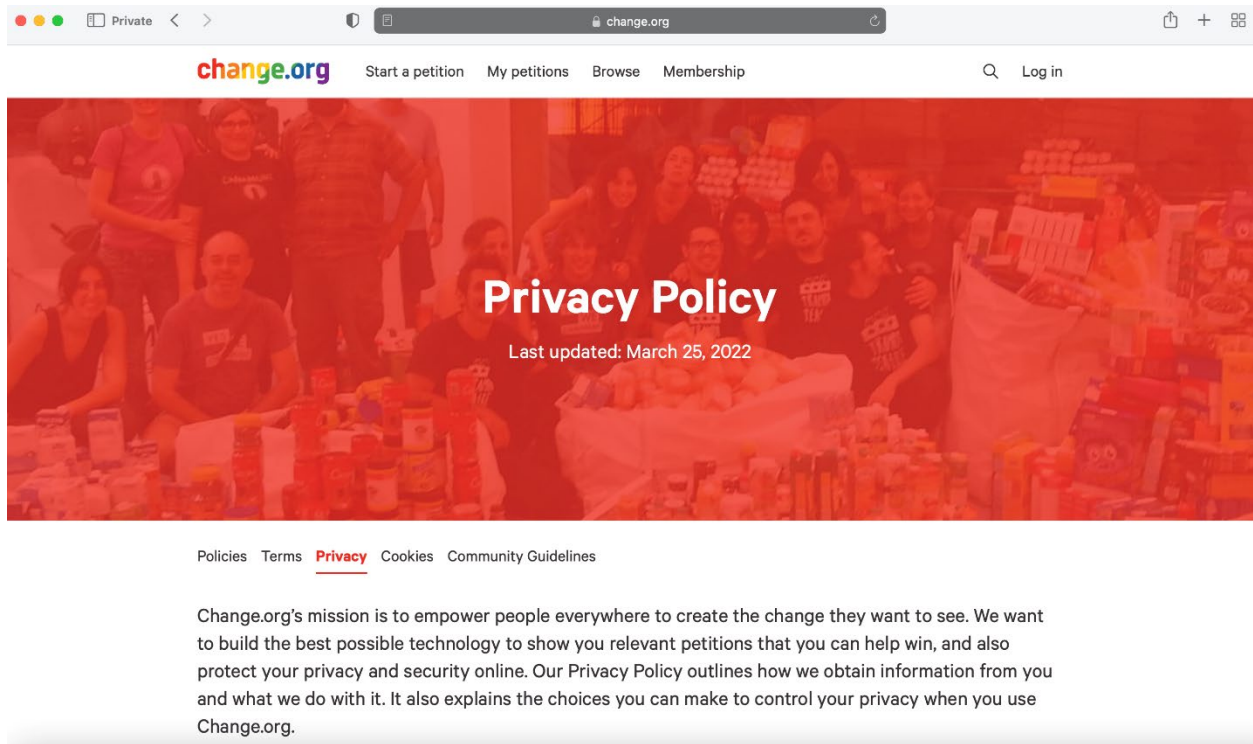
**Change.org - Chrome**



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.2.2**

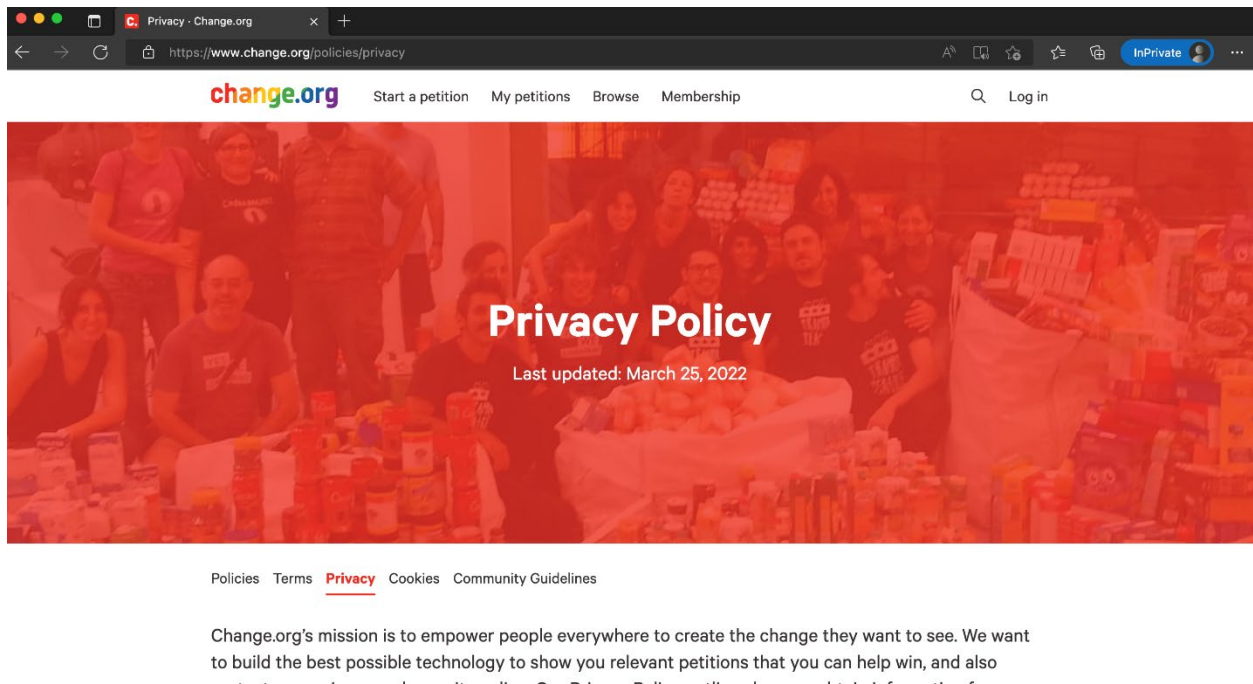
**Change.org - Safari**



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.2.3**

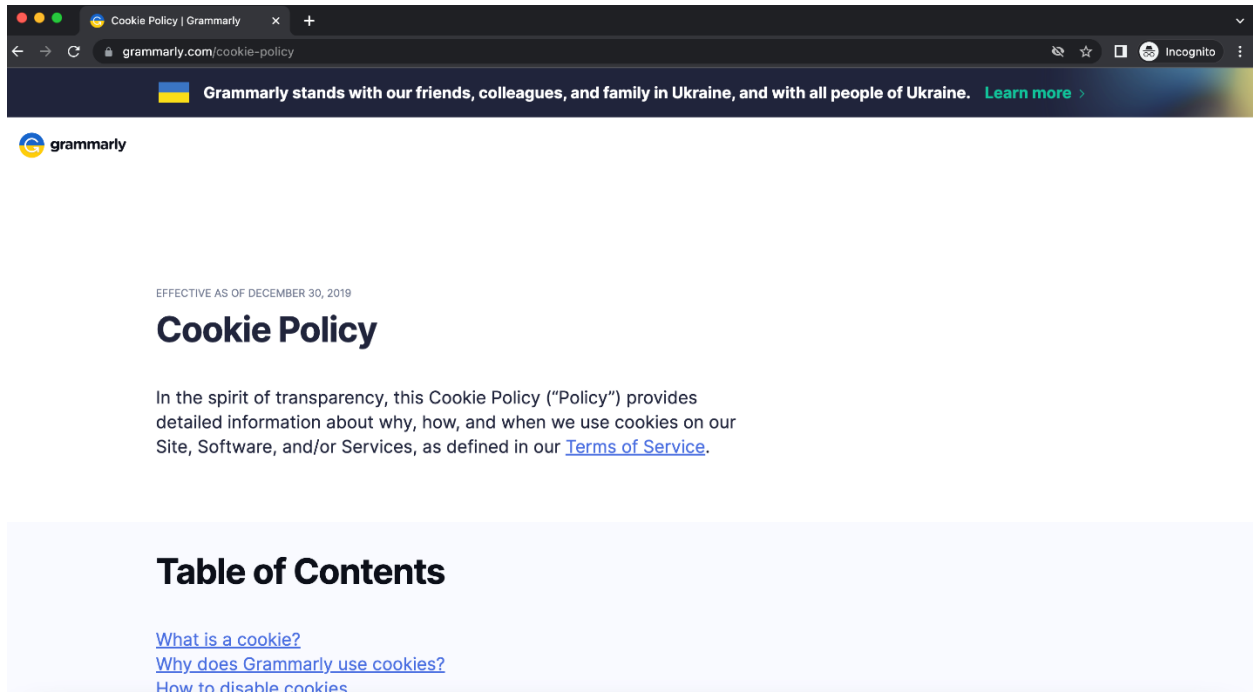
**Change.org - Edge**



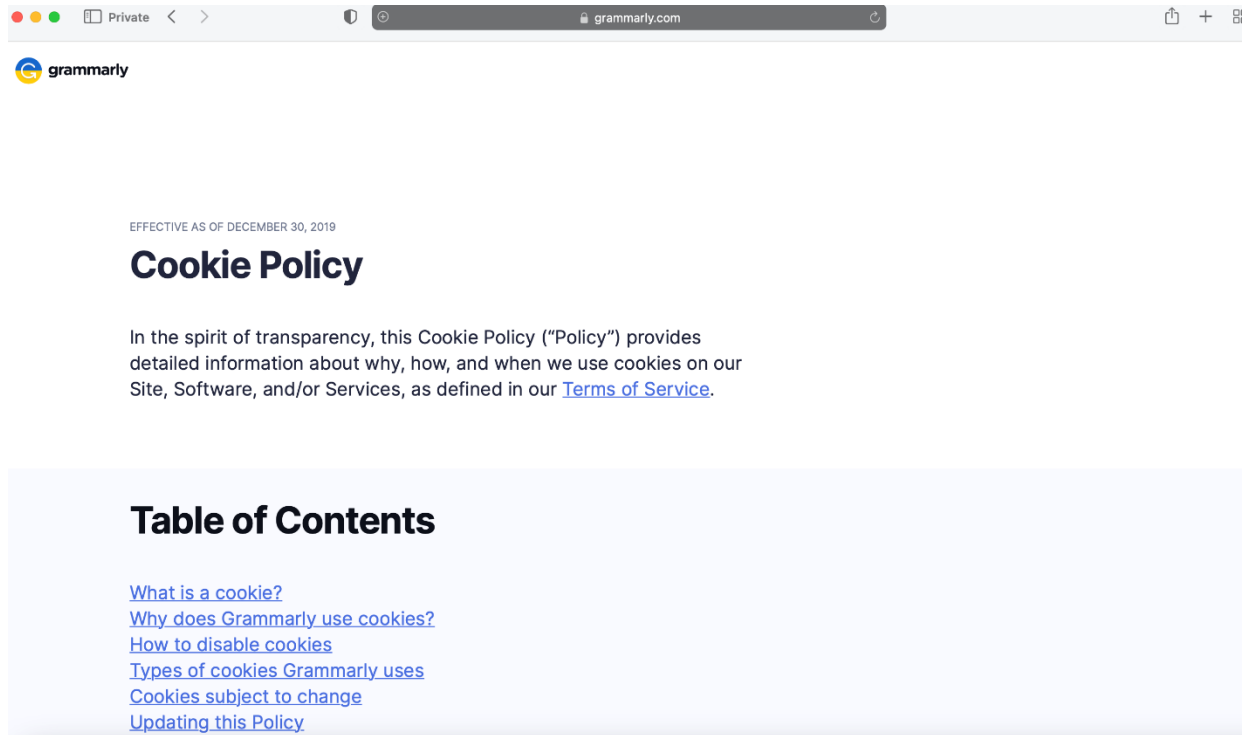
CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.3.1**

**Grammarly.com - Chrome**



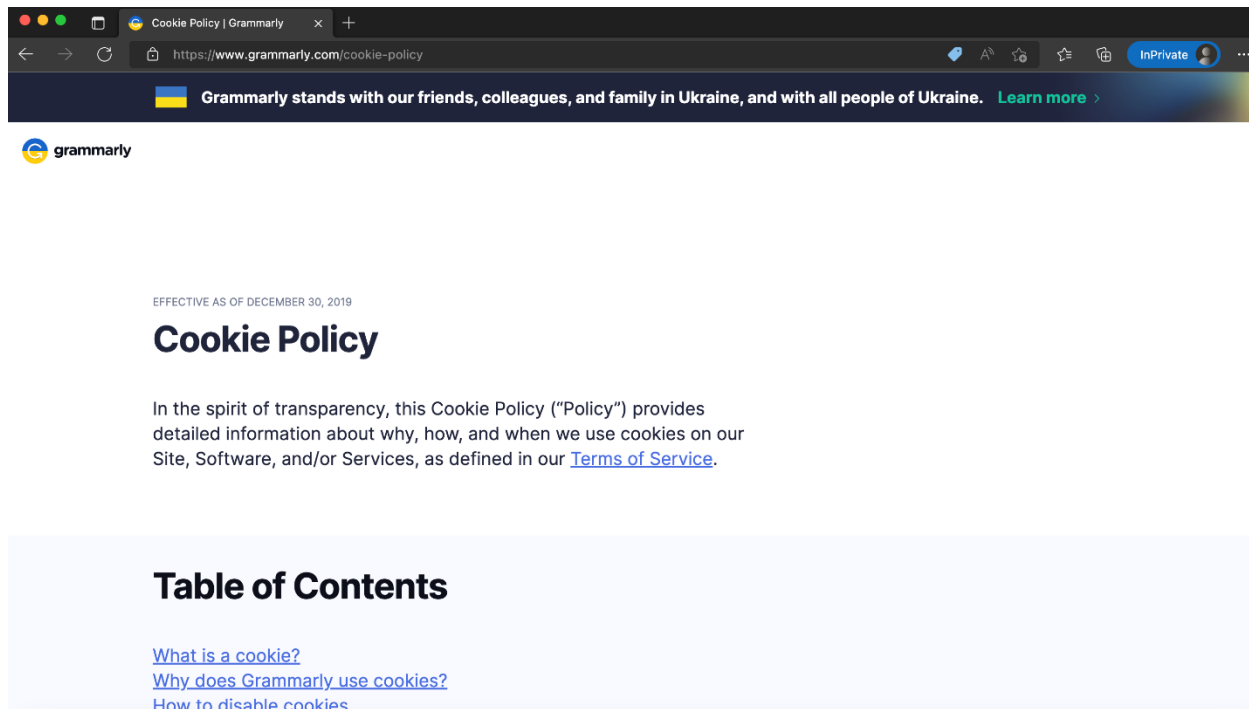
CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.3.2****Grammarly.com - Safari**

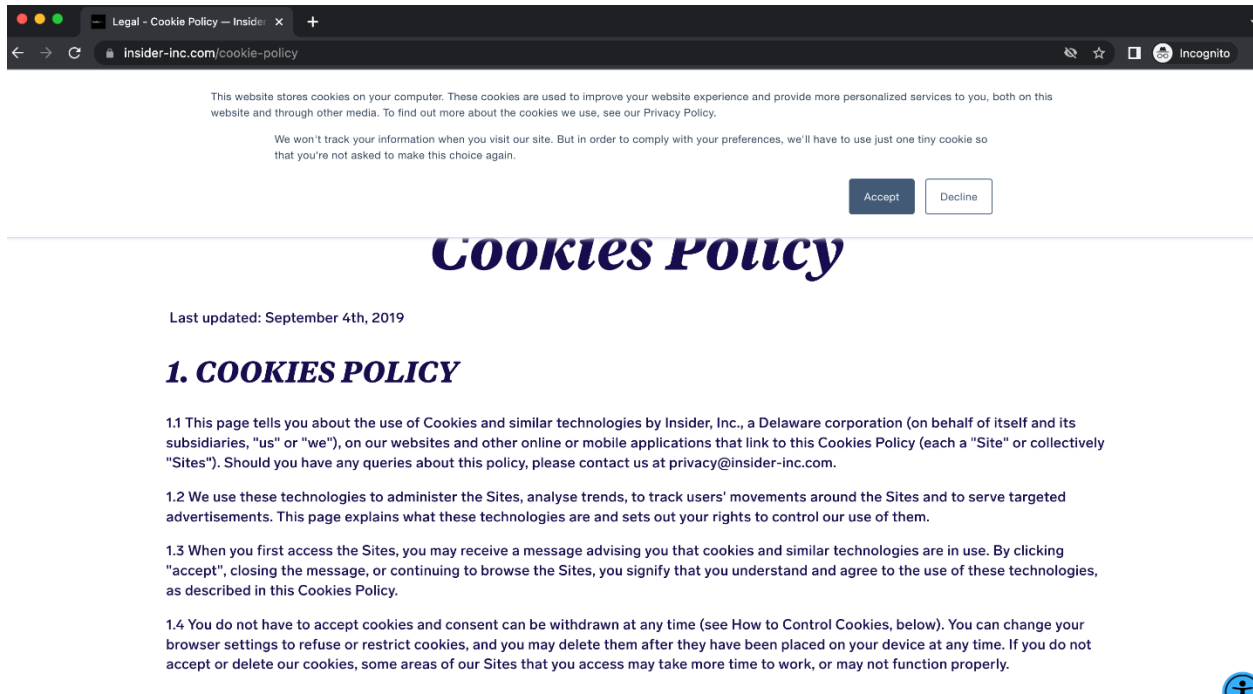
CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.3.3**

**Grammarly.com - Edge**



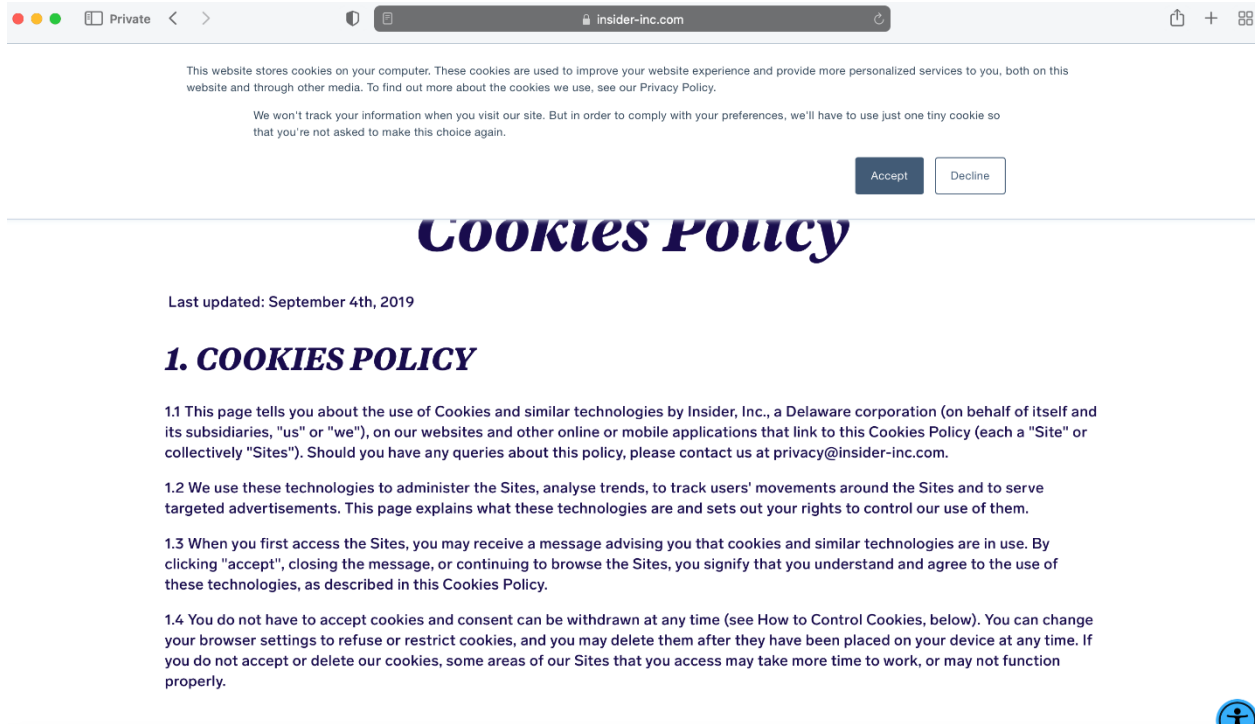
CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.4.1****Insider-Inc.com - Chrome<sup>5</sup>**

<sup>5</sup> Insider, Inc. is the owner of the *businessinsider.com* website.



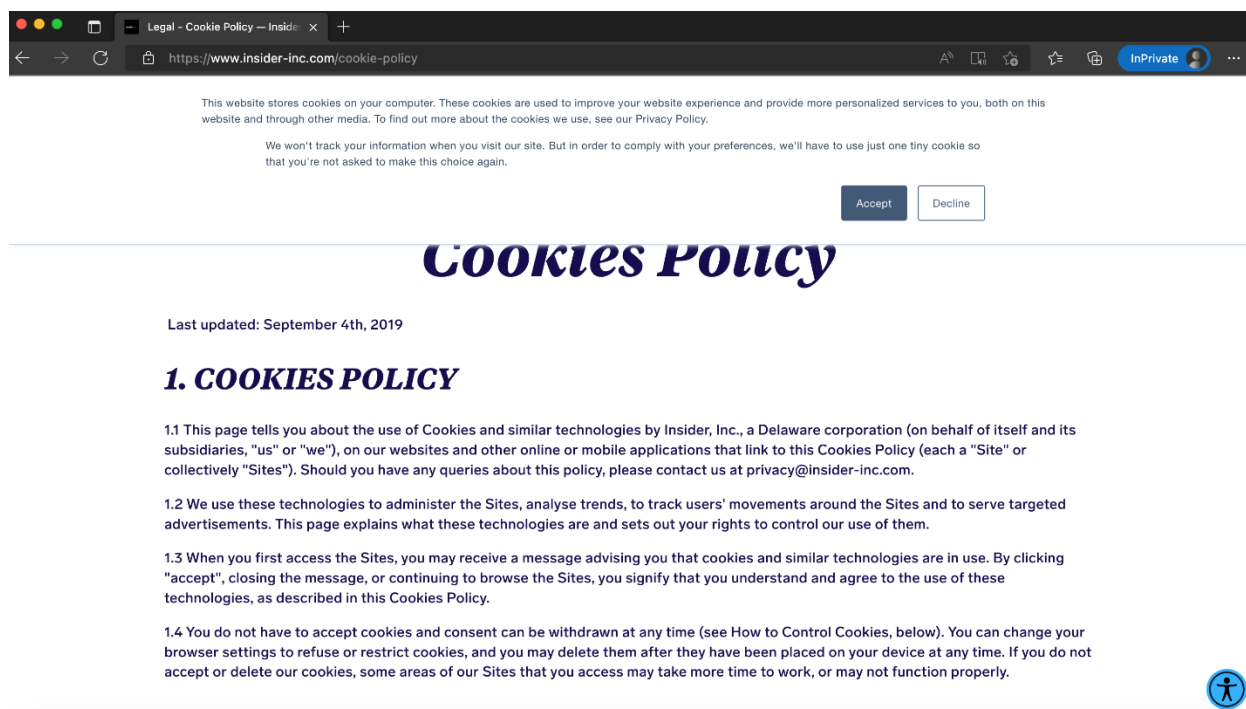
CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.4.2****Insider-Inc.com - Safari<sup>6</sup>**

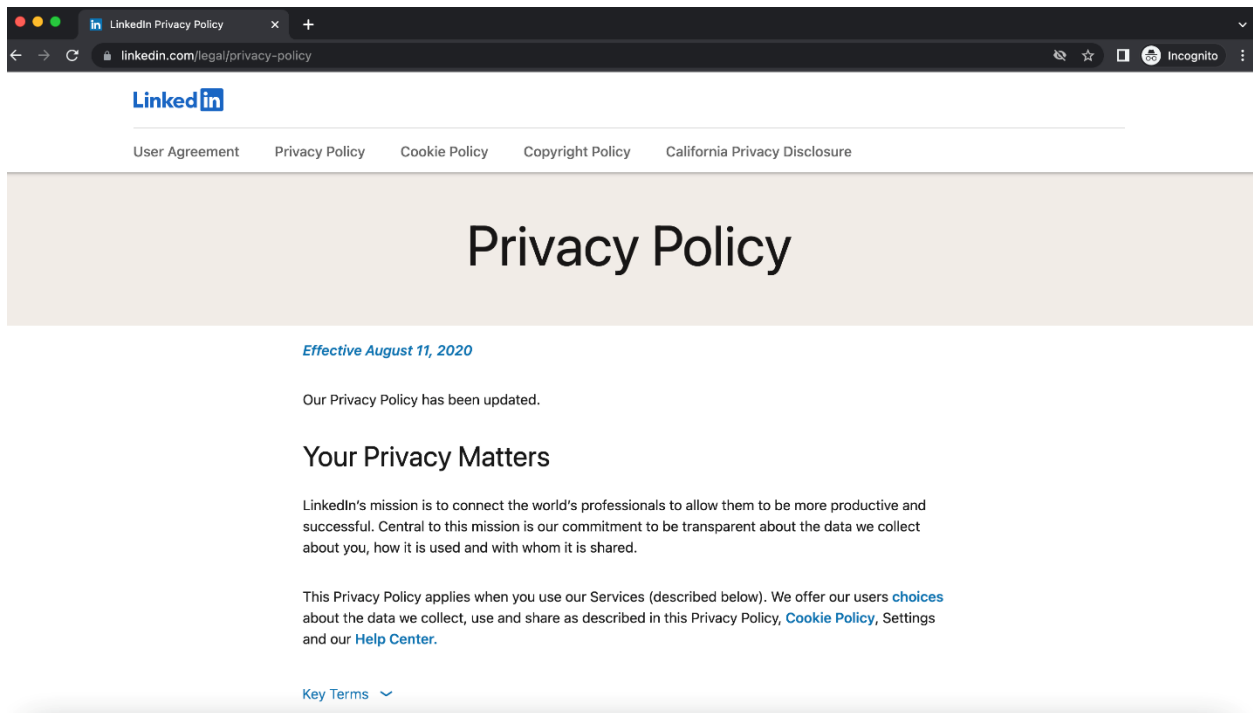
<sup>6</sup> *Insider, Inc.* is the owner of the *businessinsider.com* website.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

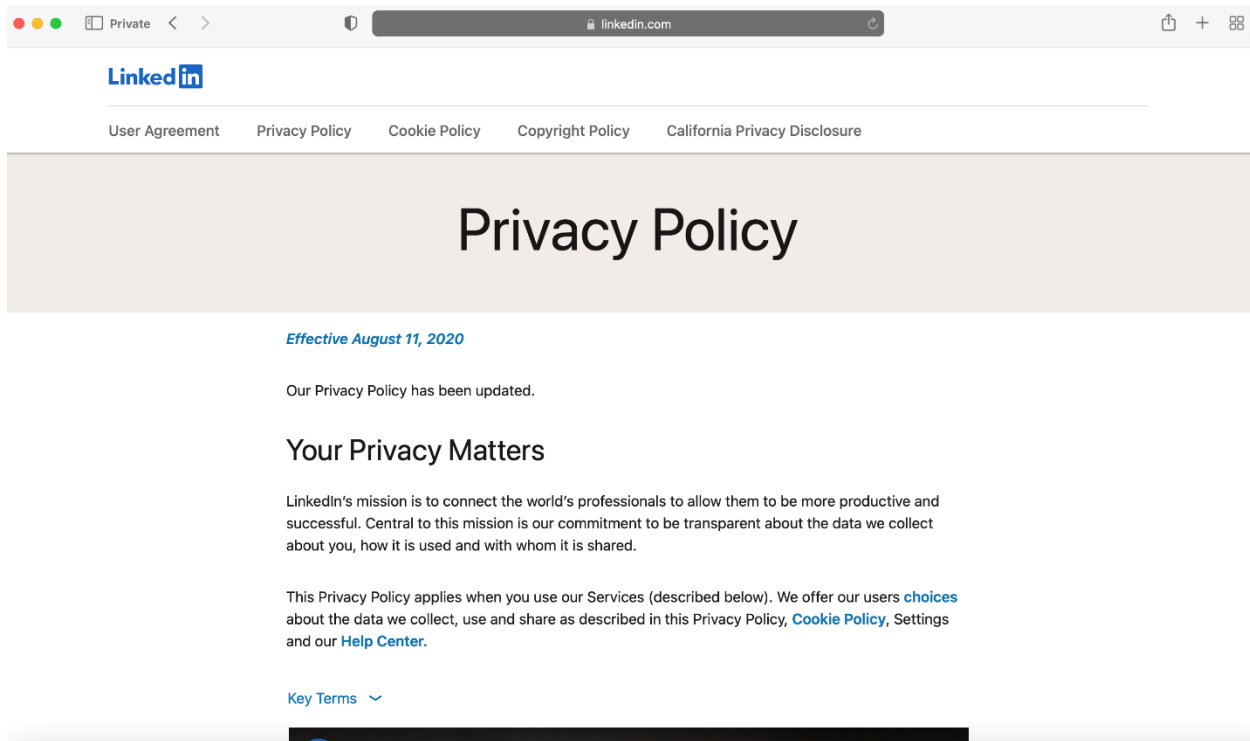
Figure D.4.3

**Insider-Inc.com - Edge<sup>7</sup>**<sup>7</sup>Insider, Inc. is the owner of the *businessinsider.com* website.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.5.1****LinkedIn.com - Chrome**

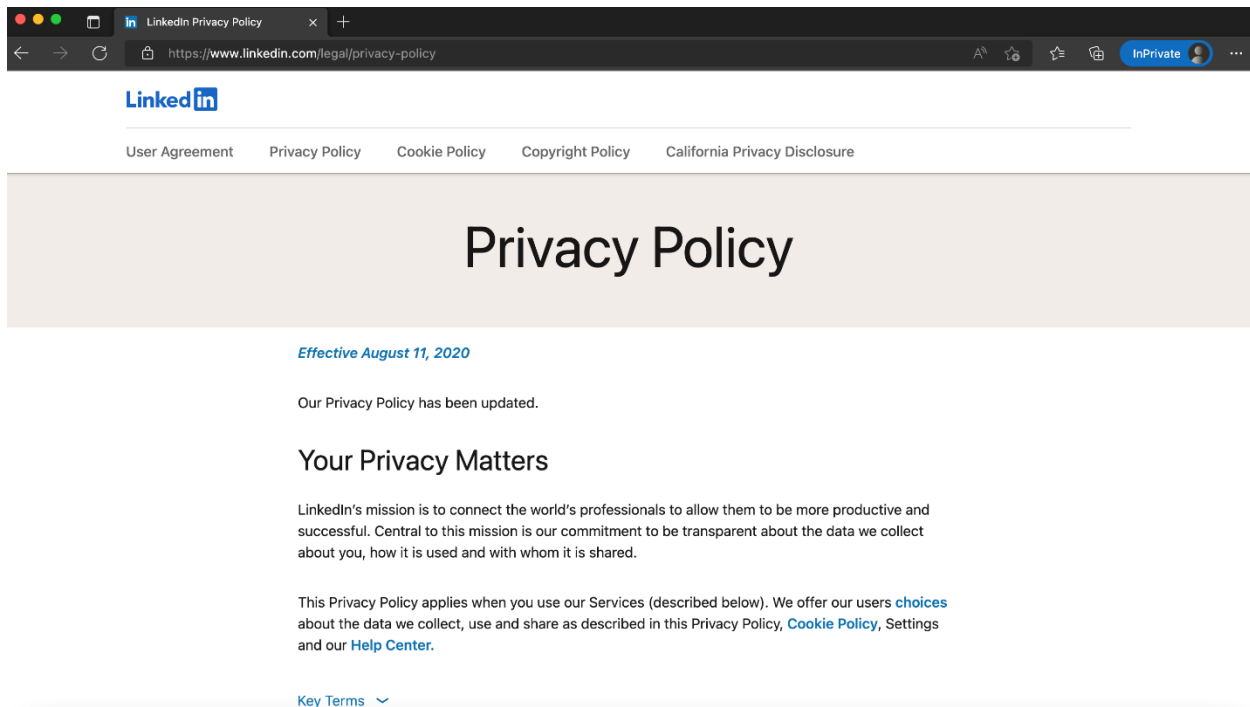
CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.5.2****LinkedIn.com - Safari**

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Figure D.5.3

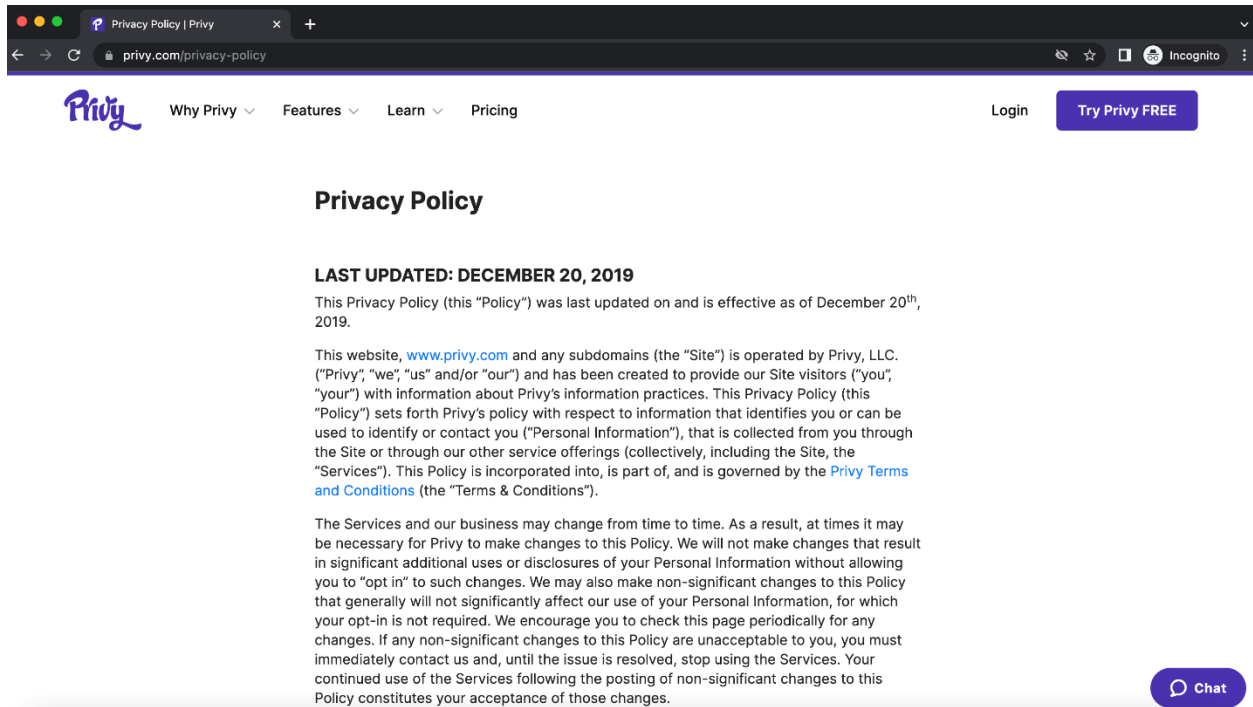
## LinkedIn.com - Edge



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Figure D.6.1

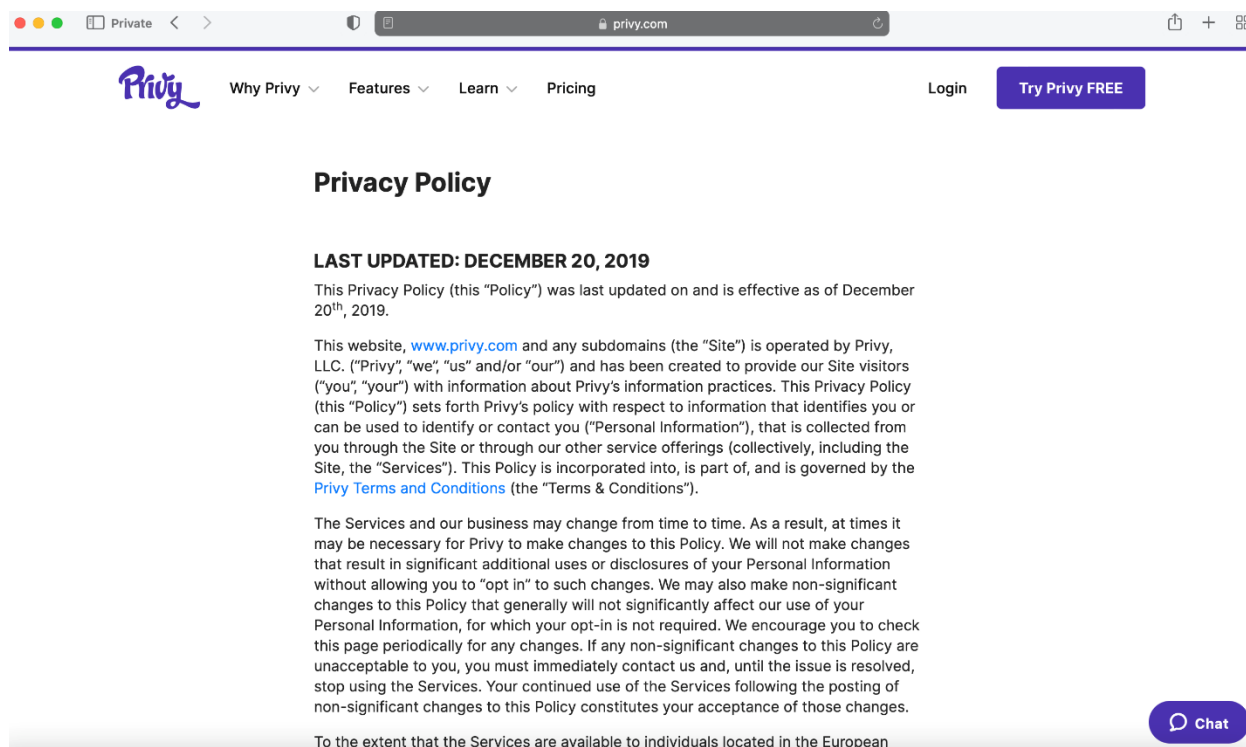
## Privy.com - Chrome



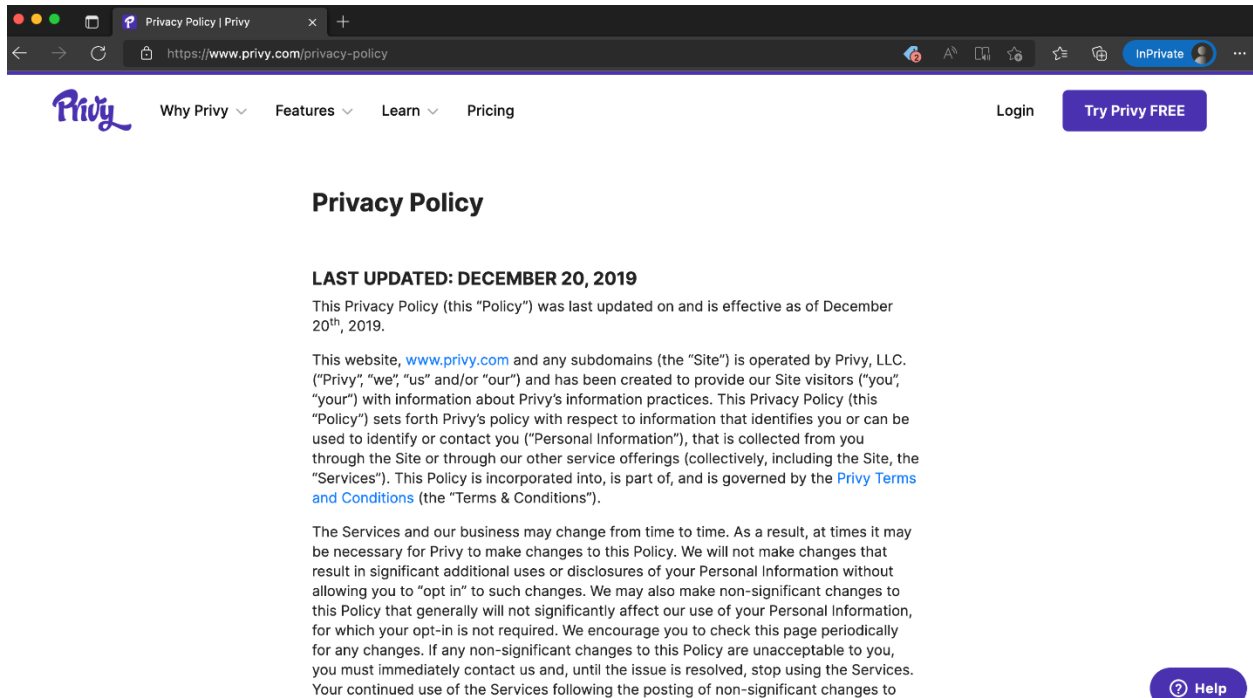
CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Figure D.6.2

## Privy.com - Safari

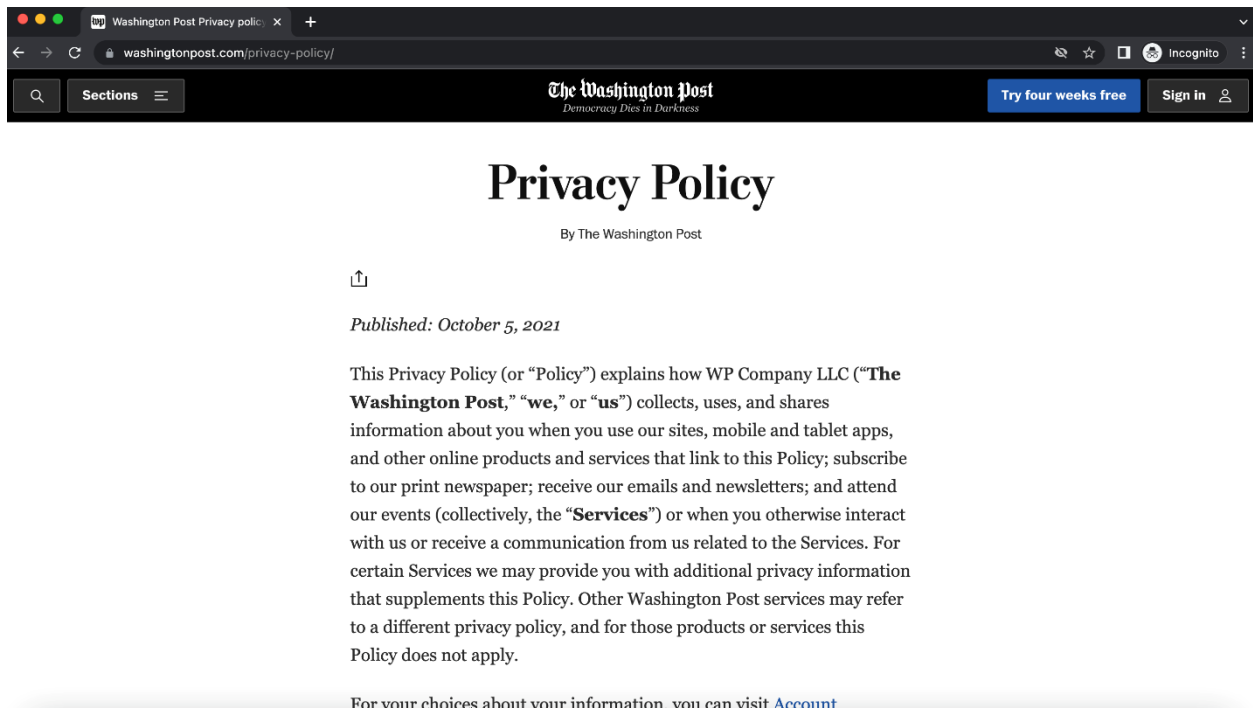


CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

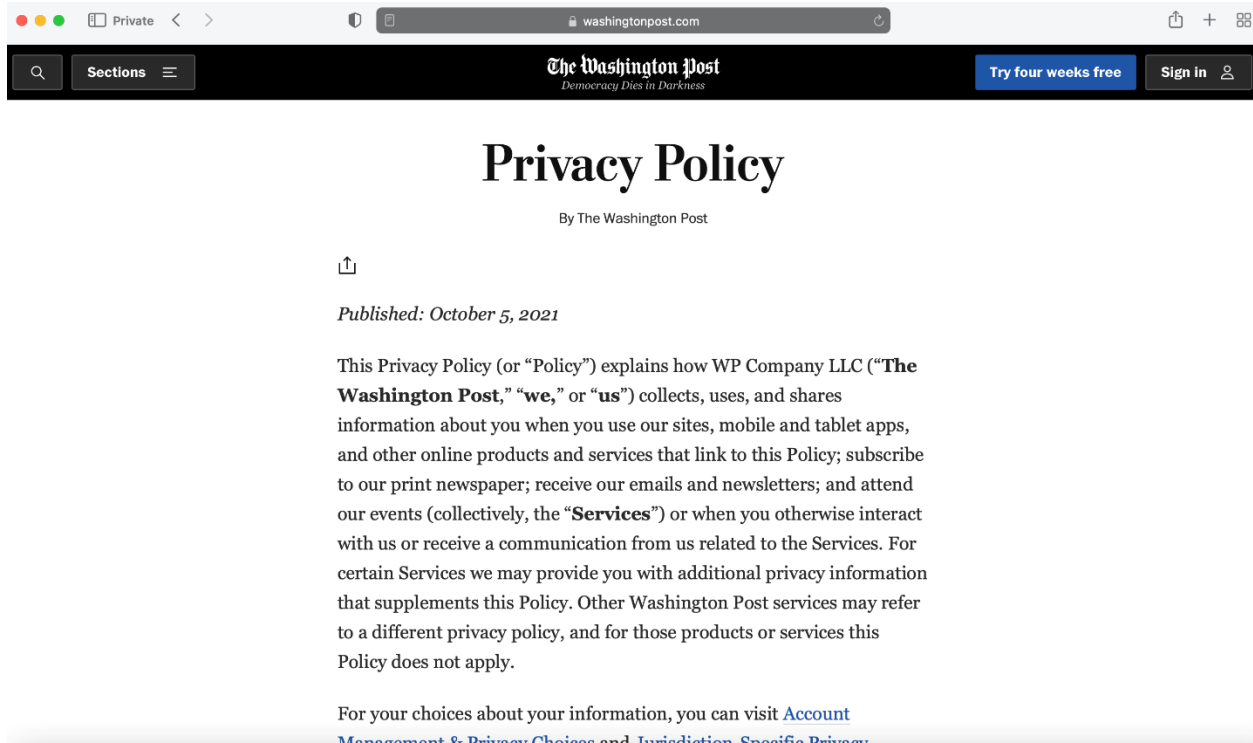
**Figure D.6.3****Privy.com - Edge**



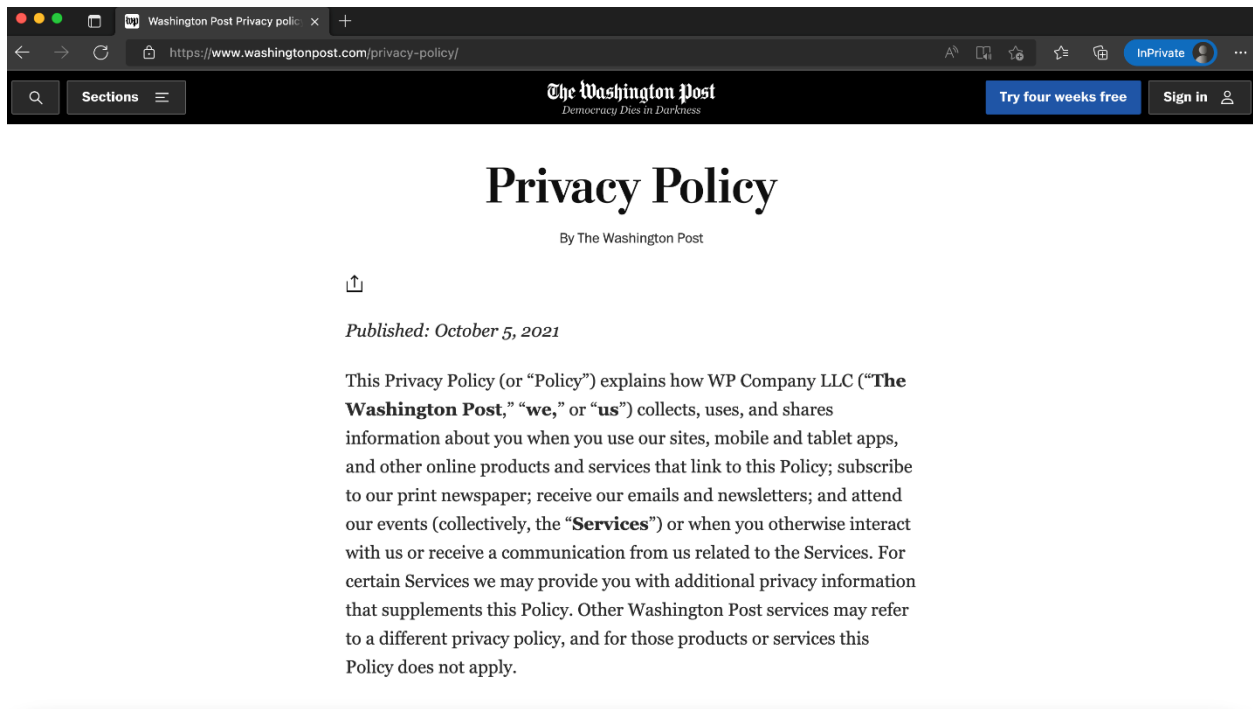
CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.7.1****WashingtonPost.com - Chrome**

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.7.2****WashingtonPost.com - Safari**

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**Figure D.7.3****WashingtonPost.com - Edge**

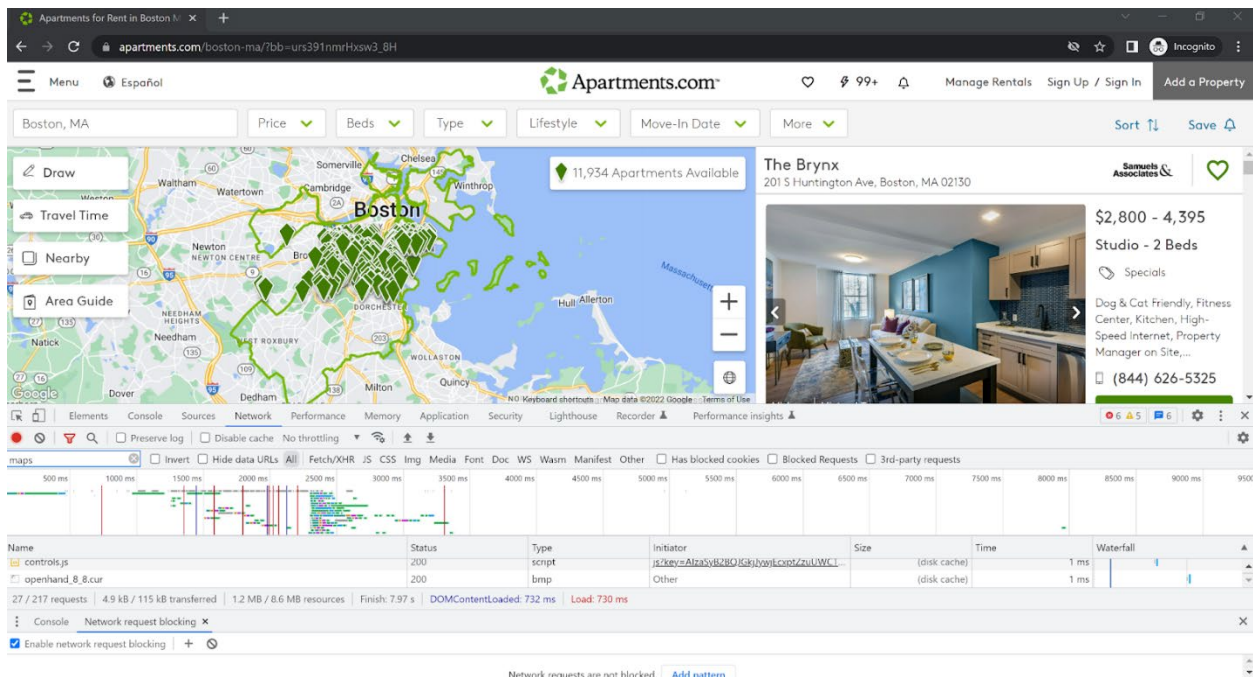
CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

## Appendix E

### Illustration Of Website With And Without Third-Party APIs

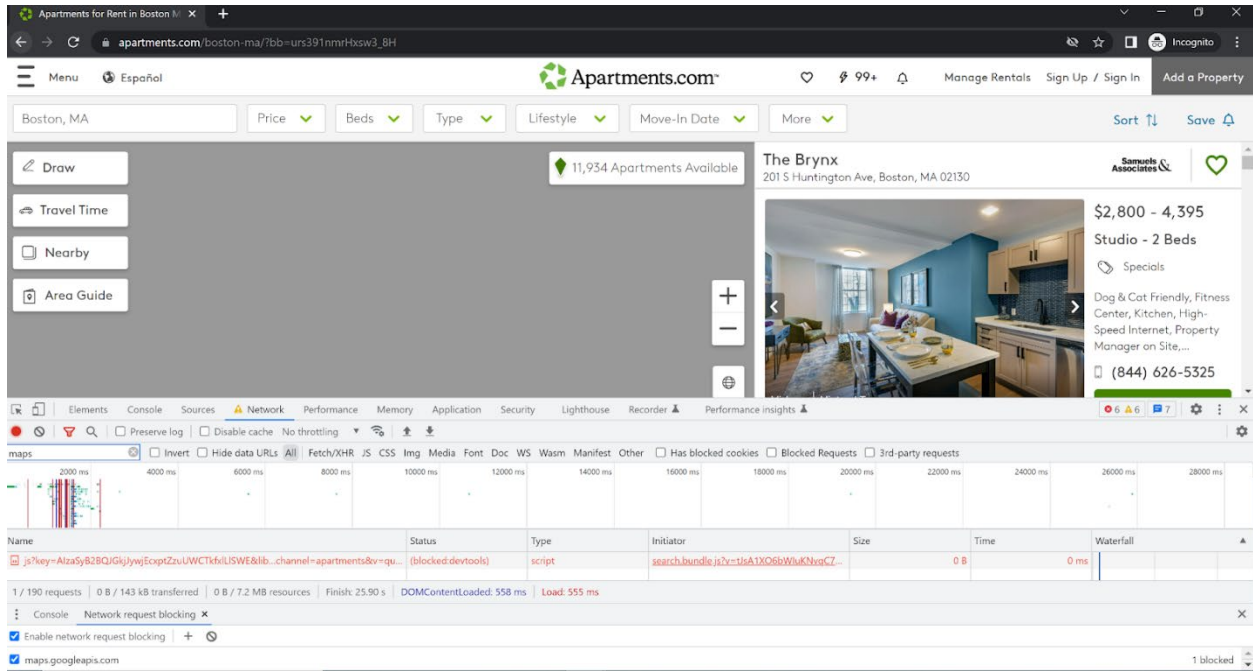
Figure E.1

#### Apartments.com *With* Google Maps API



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Figure E.2

**Apartments.com Blocking Google Maps API**

# **EXHIBIT 81**

## **6/7/22 EXPERT REPORT OF PROF. PAUL SCHWARTZ**

**Redacted Version  
of Document  
Sought to be Sealed**

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA – OAKLAND DIVISION**

CHASOM BROWN, WILLIAM BYATT,  
JEREMY DAVIS, CHRISTOPHER  
CASTILLO, and MONIQUE TRUJILLO,  
individually and on behalf of all similarly  
situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 4:20-cv-03664-YGR-SVK

**EXPERT REPORT OF PROFESSOR PAUL SCHWARTZ**

**June 7, 2022**

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
I. Executive Summary Of Opinions. ....	1
II. Personal Background And Qualifications.....	3
III. My Assignment.....	7
IV. Opinion # 1: Mr. Hochman’s Opinions Are Contrary To Information Privacy Standards.....	11
A. Mr. Hochman Fails To Distinguish Between Non-Identifying Data And Data That Is Reasonably Likely To Identify.....	11
B. Mr. Hochman’s Opinions On PI, PII, And Identifying Information Are Contrary To Information Privacy Standards In The United States.....	16
i. FTC Privacy Framework And Guidance. ....	17
ii. ALI Data Privacy Principles. ....	19
iii. CCPA’s Definitions Of “Personal Information”.....	22
V. Opinion # 2: Mr. Schneier’s Opinions On PI, PII, And Identifying Information Are Similarly Defective And Also Suffer From Additional Deficiencies Due To An Over-Inclusive Framework Where Virtually Any Data Can Be Deemed PII.....	27
VI. Opinion # 3: Mr. Hochman And Mr. Schneier Have Classified The Data At Issue Incorrectly. ....	32
A. Mr. Hochman And Mr. Schneier Fail To Take Into Account Google’s Policies And Procedures Related To Classifying The Data At Issue. ....	32
i. Google’s Privacy Policy. ....	34
ii. Google’s Data Categorization Guidelines. ....	35
iii. Google’s Anti-Fingerprinting Policy. ....	37
iv. Google’s Policies Against Re-Identifying Individuals. ....	39
B. The Data At Issue Is Not Personally Identifying, Has A Low Probability Of Identification, And Is Exempt From Data Subject Access Rights.....	41
i. The Data At Issue Is Not Reasonably Linkable Under FTC Guidance. ....	41
ii. Under ALI Principles, There Is A Low Probability That Google Could Link The Data At Issue To A Specific Natural Person. ....	43
iii. The Data At Issue Is Exempt From Certain Breach Notification Requirements, Portability, and Access and Correction Rights. ....	44
C. Individualized Determinations Would Be Required In Any Attempt To Establish That The Data At Issue Is PI Or PII. ....	46



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

## I. Executive Summary Of Opinions.

1. After reviewing Jonathan E. Hochman and Bruce Schneier’s expert reports, I have reached the following conclusions based on my expertise in information privacy principles, regulations, FTC guidance, and existing standards:

2. **Opinion # 1: Mr. Hochman’s opinions on PI, PII, and identifying information are contrary to U.S. information privacy standards.** Mr. Hochman adopts definitions of PI, PII, and identifying information, which are far-reaching, indeterminate, and contrary to U.S. information privacy standards, including (1) guidance from the Federal Trade Commission (FTC Guidance), (2) the ALI Data Privacy Principles, and (3) the California Consumer Privacy Act (CCPA). Furthermore, Mr. Hochman’s categorical approach fails to exclude data that is non-identifying, and is therefore over-inclusive. American information privacy standards require a contextual approach to determine whether a (i) “GET request,” (ii) IP address, (iii) “fingerprint” data, (iv) “User-ID,” (v) geolocation data, and (vi) information in “Google cookies” are non-identifying or likely to identify. However, Mr. Hochman fails to conduct—or propose a reasonable plan to conduct—the contextual analysis required to determine whether the Data at Issue<sup>1</sup> is reasonably linkable to, or “identifying information” for, a particular individual or class member. He also fails to consider Google’s policies and guidelines that affect whether the Data at Issue can reasonably be linked to an identified individual.

---

<sup>1</sup> This term refers to the data plaintiffs claim Google improperly receives from communications between users and websites when users are in “private browsing mode” and not signed into a Google Account and visit a web-site that uses Google services (hereafter, “the Data at Issue”): (i) “GET request” sent from the user’s computer to the website; (ii) the IP address of the user’s connection to the internet; (iii) information identifying the browser software that the user is using, including any “fingerprint” data; (iv) any “User-ID” issued by the website to the user, if available; (v) geolocation of the user, if available; and (vi) information contained in “Google cookies,” which were saved by the user’s web browser on the user’s device at any prior time.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

3. **Opinion # 2: Although Mr. Schneier does not adopt Mr. Hochman’s categorical approach to PI, PII, and identifying information, his report suffers from similar defects because he opines that even if identifying information is absent, data could be identified through additional sources.** In particular, Mr. Schneier opines that PI is any information that identifies or theoretically could be linked with an individual or their household, such as name, email, social security number, internet browsing history, etc.<sup>2</sup> He also opines that non-PII can turn into PII “whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available [non-PII] information, could be used to identify an individual.”<sup>3</sup> By ignoring Google’s practices, as established in publicly available policies and practices, Mr. Schneier’s approach is contrary to U.S. information privacy standards.

4. **Opinion # 3: The Data at Issue is not personally identifying, there is a low probability of identification by Google, and the Data at Issue is exempt from data subject access requests.** That Google may in some circumstances have sufficient information to identify some individuals cannot establish *on a class-wide basis* that the Data at Issue is PI, PII, or “identifying information” and there is a low probability that Google could individually identify users. Even if the plaintiffs were able to establish that it was PI or PII under certain circumstances, individualized factual inquiries would still be necessary to determine whether the Data at Issue is PI or PII for any given class member.

---

<sup>2</sup> Schneier ¶ 81.

<sup>3</sup> Schneier ¶ 80.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**II. Personal Background And Qualifications.**

5. I am the Jefferson E. Peyser Professor of Law at the University of California at Berkeley School of Law in Berkeley, California. I am also a Director of the Berkeley Center for Law and Technology (BCLT).

6. I received my law degree from Yale Law School, where I served as a senior editor of the Yale Law Journal. My undergraduate studies were at Brown University. I also carried out post-graduate legal studies in data protection law at the Johann Wolfgang Goethe University in Frankfurt-am-Main, Germany, as a fellow of the Alexander von Humboldt Foundation.

7. My scholarship examines the legal, regulatory, and policy implications of a wide variety of areas of information privacy and security. These include consumer privacy, data security breaches, spyware, cloud data, comparative privacy law, the international diffusion of privacy law, tax privacy, the conflict between privacy law and trade law, and other topics. At Berkeley Law School, I teach courses in information privacy, cybersecurity law, and tort law. I have been teaching information privacy law for thirty-four years, and I taught one of the very first courses in this area in the United States.

8. I have written several books, including the leading casebook INFORMATION PRIVACY LAW (7th ed., 2020), which is used at over twenty law schools, as well as the distilled guide PRIVACY LAW FUNDAMENTALS (6th ed., 2022). Daniel Solove, Professor of Law at George Washington University Law School, is my co-author on both of these books. My most important scholarly publications regarding information privacy include: *Privacy and/or Trade*, 90 UNIVERSITY CHICAGO L. REV. – (forthcoming 2023) (co-author Anupam Chander); *ALI Data Privacy: Overview and Black Letter Text*, 68 U.C.L.A. L. Rev. 1252 (2021) (co-author Daniel Solove); *Global Data Privacy: the EU Way*, 94 N.Y.U. LAW REVIEW 771 (2019); *Legal Access to*

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

*Global Cloud Data*, 118 COLUMBIA LAW REVIEW 1681 (2018); *Transatlantic Data Privacy Law*, 106 GEORGETOWN LAW JOURNAL 115 (2017) (co-author Karl-Nikolaus Peifer); *Reconciling Personal Information in the U.S. and EU*, 102 CALIFORNIA LAW REVIEW 877 (2014) (co-author Daniel Solove); *The EU-U.S. Privacy Collision*, 126 HARVARD LAW REVIEW 1966 (2013); *Information Privacy in the Cloud*, 161 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 1623 (2013); *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. LAW REVIEW 1814 (2011) (co-author Daniel Solove); *Preemption and Privacy*, 118 YALE LAW JOURNAL 902 (2009); and *Property, Privacy, and Personal Data*, 117 HARVARD LAW REVIEW 2056 (2004).

9. My scholarship is often cited as an authority on data privacy. For example:
  - My 2004 Harvard Law Review article, *Property, Privacy, and Personal Data*, was cited in plaintiffs' Complaint (see Second Amended Complaint ¶ 125, *Brown v. Google*, 5:20-cv-03664-LHK (2021), Dkt. 136-1; Third Amended Complaint ¶ 125, *Brown v. Google*, 5:20-cv-03664-YGR (2022), Dkt. 395-2). This same article was also cited in plaintiffs' Complaints in *Calhoun v. Google*,<sup>4</sup> and by plaintiffs in *In re: Facebook, Inc. Internet Tracking Litigation*, 2012 WL 12369553 at ¶ 114 (N.D. Cal. May 23, 2012).
  - My co-authored 2011 N.Y.U. Law Review article, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, was cited in the 2012 FTC Report, "Protecting Consumer Privacy in an Era of Rapid Change."<sup>5</sup>

---

<sup>4</sup> *Calhoun v. Google*, 4:20-cv-05146-YGR-SVK Dkt. 1 ¶ 215; Dkt. 163 ¶ 218; Dkt. 302-3 ¶ 213.

<sup>5</sup> Federal Trade Commission (F.T.C.) Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, 20, n.107 (March 26, 2012), <https://perma.cc/L2LX-4LEC>, citing Paul M. Schwartz & Daniel J. Solove, *The PII Problem*:

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

10. My expert opinions have been solicited in matters in federal and state courts in the United States. Google also engaged me to serve as an expert in the related case, *Calhoun v. Google*. In December 2021, I submitted an expert report in *Calhoun* responding to the information-privacy related opinions of the plaintiffs' expert, Dr. Zubair Shafiq, who was writing in support of plaintiffs' motion for class certification.<sup>6</sup> I also provided deposition testimony as an expert in the *Calhoun* matter.

11. In a past engagement, the Commissioner of Insurance of the State of California engaged me as a privacy expert to assist in litigation defending a California law, the Holocaust Victim Insurance Relief Act of 1999 (HVIRA). My expert activity on this matter included assisting the State of California with an affidavit supporting the HVIRA and explaining why, in my judgment, German data protection law did not prohibit the insurance companies in that matter from sharing insurance information pursuant to this statute. The United States Supreme Court ultimately invalidated HVIRA as a violation of the federal foreign affairs power.<sup>7</sup>

12. I have testified before the U.S. Congress, the California State Assembly, and served as an advisor to the Commission of the European Union and other international organizations. In 1990, I became the first American to address the annual meeting of the world's data protection commissioners, the International Conference of Data Protection and Privacy Commissioners (now

---

*Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814, 1836–1848 (2011).

<sup>6</sup> Because Mr. Hochman's and Mr. Schneier's reports recapitulate many of Dr. Shafiq's arguments regarding personal information and personally identifiable information, I have drawn on my previous report in *Calhoun v. Google* to rebut their arguments. See 5:20-cv-05146-LHK, Dkt. 430-1, Exhibit 3 (hereinafter, "*Calhoun* Rebuttal Report").

<sup>7</sup> See *American Ins. Ass'n v. Garamendi*, 539 U.S. 396 (2003).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

called the Global Privacy Assembly). My presentation on the state of American privacy law was delivered at their conference held in the French Senate in Paris.

13. I have testified before the California Assembly in an Informational Hearing concerning “Balancing Privacy and Opportunity in the Internet Age,” held on December 12, 2013 at the University of Santa Clara. My writings and classes have examined many questions involving California privacy law. *See, e.g.*, DANIEL SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 102-106; 821-832; 970-973 (7th ed. 2020); Paul Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 816-817 (2019); *Foreword*, in LOTHAR DETERMANN, CALIFORNIA PRIVACY LAW xxv (4th ed. 2020).

14. For several years, I have focused my teaching and scholarship on the California Consumer Privacy Act (“CCPA”). In addition to teaching the CCPA’s provisions in my information privacy class, cybersecurity class, and privacy seminar, I have also discussed it in recent articles, such as *ALI Data Privacy: Overview and Black Letter Text*<sup>8</sup> and *Global Data Privacy: The EU Way*.<sup>9</sup>

15. I am often quoted by media outlets on issues relating to privacy and technology. Publications in which I have been quoted include *The New York Times*, *the Washington Post*, *the Wall Street Journal*, *the Los Angeles Times*, *Forbes*, and *Law360*.

---

<sup>8</sup> Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA Law Review 1252 (2022), at <http://dx.doi.org/10.2139/ssrn.3457563>.

<sup>9</sup> 94 N.Y.U. Law Review 771 at 816–817 (2019).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

16. At the American Law Institute (ALI), I served as a co-reporter on the Data Privacy Principles Project.<sup>10</sup> As the ALI explains, the project seeks “to provide a framework for regulating data privacy and for duties and responsibilities—best practices—for entities that process personal data.”<sup>11</sup> Founded in 1923, the ALI is “the leading independent organization in the United States producing scholarly work to clarify, modernize, and otherwise improve the law.”<sup>12</sup> Over the course of its history, the ALI has been responsible for such major path-breaking projects as the Restatement of Torts, the Uniform Commercial Code, the Model Penal Code, and the Principles of Corporate Governance.

### III. My Assignment.

17. I have been retained by Defendant Google, LLC in the above-captioned matter to evaluate certain sections of the reports of plaintiffs’ experts, Jonathan E. Hochman and Bruce Schneier. The first opinion of my report addresses Mr. Hochman’s conclusions regarding *personal information* (“PI”), *personally identifiable information* (“PII”), *identifying information, entropy, and fingerprinting*,<sup>13</sup> which are relevant to Opinions 2, 9, 10, 14, and 22 of his report. The second opinion of my report addresses Mr. Schneier’s conclusions regarding PI, PII, identifying information, and fingerprinting. The second opinion relates to Opinions 3, 7, 8, and 9

---

<sup>10</sup> See The American Law Institute, “Principles of the Law: Data Privacy” (<https://perma.cc/986V-87QA>); see also Solove, Daniel J. and Schwartz, Paul M., *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA Law Review 1252 (2022).

<sup>11</sup> The American Law Institute, “Principles of the Law: Data Privacy” (<https://perma.cc/986V-87QA>).

<sup>12</sup> *About ALI*, The American Law Institute (2022), <https://www.ali.org/about-ali/>.

<sup>13</sup> “[F]ingerprinting is the use of unique or probabilistically unique combinations of one or more device, network, or app/browser attributes to identify a device, app, browser, or user across distinct transactions where no persistent unique identifier is explicitly provided by a user’s device, app, or browser.” GOOG-CALH-00027147 (Privacy Policy – Device/App/Browser Fingerprinting and Immutable Identifiers Policy).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

of Mr. Schneier’s report. The third opinion rebuts the analysis Mr. Hochman and Mr. Schneier applied and analyzes the Data at Issue under the correct U.S. information privacy standards. The third opinion concludes that the Data at Issue in this litigation is not personally identifying; there is a low probability of Google identifying users from the Data at Issue; and the Data at Issue is exempt from certain data breach notice requirements as well as data subject access rights. The third opinion explains that to rebut the conclusion that the Data at Issue is not PII, individualized determinations would be required to establish the probability that Mr. Hochman’s proposed “fingerprinting” would allow for particular users to be identified.

18. I understand that expert Georgios Zervas will discuss Mr. Hochman’s opinions relating to descriptions of Google’s web services and client-side data practices (Opinions 1, 2, 3, 4, 5, 6, 10, 15, 26, 27, 28, and 29) and expert Konstantinos Psounis will rebut Mr. Hochman and Mr. Schneier’s opinions regarding Google’s server-side data practices (Mr. Hochman Opinions 4, 5, 6, 9, 10, 14, 18, 19, 20, 22, 23, 24, 26, and 31; Mr. Schneier Opinions 3, 6, 9).

19. With respect to the class action litigation, I understand that plaintiffs Chasom Brown, William Byatt, Jeremy Davis, Christopher Castillo, and Monique Trujillo allege that Google violated various statutes and privacy laws. Specifically, plaintiffs allege that Google “unlawfully intercepted users’ private browsing communications to collect personal and sensitive information ... without disclosure or consent.”<sup>14</sup> Plaintiffs claim that “Google intercepts and collects this data by causing the user’s web browsing software to run Google software scripts ... that replicate and send the data to Google servers ... even if the user is not engaged with any Google site or functionality and even when the user is in a private browsing mode ... [without]

---

<sup>14</sup> TAC ¶ 4.



## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

notice to the user of Google’s data collection methods.”<sup>15</sup> Plaintiffs further allege that Google’s receipt of certain categories of information gives rise to liability, including unauthorized disclosure, breach of contract, invasion of privacy, theft, and unauthorized access of personal information. A purported violation of the CCPA is not one of plaintiffs’ causes of action. The CCPA is referenced throughout the Complaint and by plaintiffs’ experts, however, and I will therefore discuss it as one of several standards for determining whether data should be considered to be “personal information.”

20. Plaintiffs claim that “Google has gained a complete cradle-to-grave profile of users” by “tracking, collecting and intercepting users’ (including plaintiffs’ and class members’) personal communications indiscriminately[.]”<sup>16</sup> Plaintiffs claim that Google improperly receives the following types of data from communications between users and websites when users are in “private browsing mode” and not signed into a Google Account and visit a web-site that uses Google services (as indicated above, “the Data at Issue”): (i) a “GET request” sent from the user’s computer to the website; (ii) the IP address of the user’s connection to the internet; (iii) information identifying the browser software that the user is using, including any “fingerprint” data; (iv) any “User-ID” issued by the website to the user, if available; (v) geolocation of the user, if available; and (vi) information contained in “Google cookies,” which were saved by the user’s web browser on the user’s device at any prior time.<sup>17</sup>

21. Plaintiffs further allege that the “[i]nformation collected from Google Cookies ... includes identifying information regarding the user from private browsing sessions and non-private

---

<sup>15</sup> TAC ¶ 5.

<sup>16</sup> TAC ¶ 93.

<sup>17</sup> TAC ¶ 63 (emphasis added).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

browsing sessions, across multiple sessions.”<sup>18</sup> Plaintiffs also allege that Google collects “[i]dentifying information regarding the consumer from various Google fingerprinting technologies that uniquely identify the device, such as X-Client-Data Header, GStatic, and Approved Pixels.”<sup>19</sup>

22. I understand that plaintiffs are proposing two classes for this lawsuit:

**Class 1** – All Chrome browser users with a Google account who accessed a non-Google website containing Google tracking or advertising code using such a browser and who were (a) in “Incognito mode” on that browser and (b) were not logged into their Google account on that browser, but whose communications, including *identifying information* and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present (the “Class Period”).

**Class 2** – All non-Chrome browser users with a Google account who accessed a non-Google website containing Google tracking or advertising code using any such browser and who were (a) in “private browsing mode” on that browser, and (b) were not logged into their Google account on that browser, but whose communications, including *identifying information* and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present (the “Class Period”).<sup>20</sup>

23. I am being compensated for my work at the rate of \$1,215 per hour. My opinions in this matter are in no way dependent on my compensation or the outcome of this case.

---

<sup>18</sup> *Id.* ¶ 93 (emphasis added).

<sup>19</sup> *Id.* ¶ 93 (emphasis added).

<sup>20</sup> TAC ¶ 192.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

#### IV. **Opinion # 1: Mr. Hochman’s Opinions Are Contrary To Information Privacy Standards.**

##### A. **Mr. Hochman Fails To Distinguish Between Non-Identifying Data And Data That Is Reasonably Likely To Identify.**

24. Mr. Hochman’s report adopts categorical definitions of PI and PII.<sup>21</sup> First, with respect to PI, Mr. Hochman claims that “URLs, IP addresses, user agent, referer, and other information from the user’s private browsing communications” are “personal information” that Google collected throughout the class period.<sup>22</sup> In a separate passage, he states that “URLs visited,” “[i]dentifiers on non-Google websites matched to Brown’s Biscotti ID,” “[d]evice type,” “[o]perating system and version,” “[b]rowser type and version,” and “[l]anguage” are also personal information that Google collected while a named Plaintiff was logged-out of their account and in private browsing mode.<sup>23</sup>

25. Second, with respect to PII, Mr. Hochman states that in his opinion “an IP address, especially when combined with a user-agent string, constitutes personally identifiable information (“PII”) because this data can be used to uniquely identify a user *with a high probability of success*.”<sup>24</sup> Then he provides a definition of PII from a blog post by Corinne Bernstein, Adjunct Assistant Professor in the Department of Humanities at Farmingdale State College: “Personally

---

<sup>21</sup> See e.g., Hochman ¶ 106 (“[T]he intercepted and collected information in private browsing mode are sensitive, personal information...that...includes data such as IP address, cookie/device ID, PII, postal address, geo-location data etc.”); ¶ 174 (“This Google file...contains a myriad of personal information and private browsing activities, including...URLs visited[,] Identifiers on non-Google websites matched to Brown’s Biscotti ID[,] Device type[,] Operating system and version[,] Browser type and version[,] Language[,] Location information including latitude and longitude[,] Travel history including number of countries, cities and airports visited[.]”).

<sup>22</sup> *Id.* ¶ 99 (emphasis added).

<sup>23</sup> *Id.* ¶ 174.

<sup>24</sup> *Id.* ¶ 105 (emphasis added).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

identifiable information (PII) is *any data that could potentially identify a specific individual*. Any information that can be used to distinguish one person from another and can be used to deanonymize previously anonymous data is considered PII.”<sup>25</sup>

26. Mr. Hochman assumes a broad and amorphous definition of PII as “any data that could potentially identify a specific individual.” In his opinion, Mr. Hochman focuses on a measure known as “entropy,” which—according to Mr. Hochman—calculates the “number of bits of data needed to uniquely identify a person.”<sup>26</sup> In Mr. Hochman’s opinion, the number of required bits globally is 33 “[w]ith a little less than 8 billion people on earth” and “[w]ith around 330 million people in the United States, 29 bits of data is more than sufficient to identify a person.”<sup>27</sup> For Mr. Hochman, information—or multiple pieces of information put together—that reach or exceed 29 bits are sufficient to identify an individual in the United States.<sup>28</sup> Under Mr. Hochman’s entropy approach, the Data at Issue is therefore PII if it reaches or exceeds a specific threshold (*i.e.*, 29) that can be mathematically calculated.<sup>29</sup>

---

<sup>25</sup> *Id.* ¶ 105 (emphasis added), citing <https://perma.cc/37V9-FZGA> (last accessed on May 11, 2022) (“[PII] may include the following: name, address, email, telephone number, date of birth, passport number, fingerprint, driver’s license number, credit or debit card number, Social Security number”).

<sup>26</sup> *Id.* ¶ 231.

<sup>27</sup> *Id.*

<sup>28</sup> *See id.*

<sup>29</sup> In support of *Calhoun* plaintiffs’ motion for class certification, Dr. Zubair Shafiq submitted an expert report in which he opines that the Data “uniformly” sent from Chrome to Google at issue in the case is “PI” and “PII.” In a similar approach to Mr. Hochman, Dr. Shafiq defines PII by calculating the so-called “entropy” (in bits) of the “minimum amount of information required to uniquely identify” an individual internet user on earth. According to Dr. Shafiq, that number of required bits is 32 and therefore information (“or multiple pieces of information put together”) that reaches or exceeds a “32-bit threshold” is PII. *See Calhoun v. Google*, 5:20-cv-05146-LHK, Dkt. 340-19, Report of Dr. Zubair Shafiq; *see also Calhoun* Rebuttal Report.

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

27. Finally, Mr. Hochman’s report treats “identifying information” as information that does not directly identify an individual person, but rather information that *could* be joined with other information to identify an individual. For example, Mr. Hochman acknowledges that the Data at Issue is stored in a way that is not directly linked to a person’s Google Account. However, he opines that the Data at Issue could be linked to class members with various “identifying information” such as IPv6 addresses.<sup>30</sup> Elsewhere he states that cookies—one of the types of Data at Issue—“are pieces of ‘text stored by a user’s web browser’ containing *identifying information* and used by Google for tracking and advertising purposes.”<sup>31</sup> In my opinion, Mr. Hochman’s treatment of “identifying information” is contrary to how that term is commonly defined in U.S. information privacy standards.<sup>32</sup> Mr. Hochman’s opinion in this litigation on “identifying information” is also contrary to a recent publication by Mr. Hochman, in which he states the following:

An identifier by itself is meaningless and is just a code. For example, any random combination of nine numbers very well may be a social security number, but without identifying information, there is no relevance, utility or vulnerability. Identifying information alone is not overly relevant, because it simply notes the existence of a person, without any detail of that person.<sup>33</sup>

---

<sup>30</sup> *Id.* ¶ 229 (“Within Google’s various logs and storage, IP address, particularly IPv6, can be used to link data from different logs storing signed-out data collected from private browsing and non-private browsing modes to a particular user’s device and to the user’s signed-in identity and data.”); *see also id.* ¶ 156 (“As for the private browsing information at issue in this case – where class members are not signed into any Google account – Google stores the data in a way that people have no ability to review or delete that information – with various *identifying information* that could be linked to class members and their devices.”) (emphasis added).

<sup>31</sup> *Id.* ¶ 108 (emphasis added).

<sup>32</sup> *See, e.g.*, App. C (42 C.F.R. § 426.400, 5 C.F.R. § 581.203, 34 U.S.C.A. § 12291, 22 U.S.C.A. § 2507a, 42 U.S.C.A. § 11360).

<sup>33</sup> Michael J. Fischer, Jonathon E. Hochman, and Daniel Boffa, “Privacy-Preserving Data Sharing for Medical Research,” *Stabilization, Safety, and Security of Distributed Systems*: 23rd

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

28. **There is no single definition for personal data that applies in all laws and regulations in the United States.** As a matter of comparative privacy standards, this development in the United States is quite different from the situation in the European Union, where there is a single definition of this concept.<sup>34</sup> As illustrated in Appendices A, B, and C, the United States also lacks a single term for the basic idea of personal data: personal information. Terms used to express this concept include: personal identification information, personally identifiable information, nonpublic personal information, personal health information, and electronic personal health information.

29. Increasingly, however, **the U.S. approach to information privacy generally converges around the same touchstone concept: Data falls under information privacy guidelines when it can be “reasonably linked” to an individual.**

30. Mr. Hochman’s theory, which is based on a categorical mathematical definition, is contrary to this well-established approach. Although Mr. Hochman’s report and supporting materials provide examples of myriad laws, regulations and instruments that use the terms PI and PII, none of these laws, regulations, and instruments even mention the 33-bit (global) or 29-bit (U.S.) formula that Mr. Hochman applies. I am also not aware of any privacy policy, regulation, or court in the United States applying this categorical definition of personal information.

---

International Symposium, SSS 2021, Virtual Event, [https://doi.org/10.1007/978-3-030-91081-5\\_6](https://doi.org/10.1007/978-3-030-91081-5_6) (Nov. 17–20, 2021) (“Hochman Paper”), at 2-3.

<sup>34</sup> The European Union defines “personal data” as “any information relating to an identified or identifiable natural person (‘data subject’).” General Data Protection Regulation, Article 4. For an analysis of the use of this term in the European Union, see Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Calif. L. Rev. 887, 882–87 (2014).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

31. Mr. Hochman opines that the categories of Data at Issue in this case automatically constitute PII once they reach the 33-bit (or 29) threshold, a conclusion that he reaches without contextual analysis of Google’s actual data processing practices and stated policies.<sup>35</sup> Mr. Hochman appears to believe that because the Data at Issue is complex enough that it could *theoretically* distinguish among four billion individuals, that is enough to render the Data at Issue PI or PII irrespective of any other factors, including whether Google takes steps to prevent such linking. But American information privacy standards do not support such an interpretation. On the contrary, these standards make clear that a contextual approach is required to classify the Data at Issue.

32. The critical flaw in Mr. Hochman’s approach is that it considers only a high level abstraction, namely the “amount of information”<sup>36</sup> theoretically available to Google and whether it is more or less than 29-bits in the U.S. (or 33-bits globally). This is not the correct methodology to apply in the circumstances of deciding a class certification.

33. Mr. Hochman simply considers how much data to which Google can gain access, and not what measures it may internally take to restrict, limit, or channel access to such data and the linking of that information. As a consequence, Mr. Hochman fails to consider the important issue of whether the Data at Issue could reasonably be linked to an individual in the real world, or whether impediments, including internal protocols or processes, are in place to stop such linkage.

34. Put differently, Mr. Hochman presents a *theoretical* model, and one which may be highly useful for certain experiments in the world of information theory, but fails to consider the kinds of questions on which information privacy standards typically focus. For example, Mr.

---

<sup>35</sup> Hochman ¶¶ 231-233.

<sup>36</sup> Hochman ¶¶ 166, 231.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Hochman does not look at whether the company processing the Data at Issue has implemented protocols or processes to *prevent* the Data at Issue from being reasonably linked to an individual. In the United States, such measures are a key factor when classifying data. Another common question in U.S. information privacy standards is whether there is a low, moderate, or high probability that the Data at Issue could be linked to an individual.<sup>37</sup> Because Mr. Hochman’s approach ignores these important practical considerations, it is contrary to current American information privacy principles.

**B. Mr. Hochman’s Opinions On PI, PII, And Identifying Information Are Contrary To Information Privacy Standards In The United States.**

35. Mr. Hochman’s theory of PI, PII, and identifying information is contrary to at least the following: (1) guidance from the Federal Trade Commission (FTC Guidance), (2) the ALI Data Privacy Principles, and (3) the California Consumer Privacy Act (CCPA). I draw on these three frameworks to illustrate the emerging center of gravity regarding the identifiability of data. These three frameworks are not referenced to indicate any conclusion regarding Google’s ultimate legal obligations in this case, but simply to show that Mr. Hochman’s theory of personal information conflicts with prevailing U.S. information privacy standards.

36. Even beyond the three comparisons I make below (*i.e.*, to FTC Guidance, ALI principles, and the CCPA), **the concepts of PI, PII, and “identifying information” in the United States are generally limited to instances where data refers to an *identified* individual.**<sup>38</sup> I have explored this point in a series of articles I have written with Professor Daniel Solove, the John

---

<sup>37</sup> *Infra* ¶¶ 46-50, App. C.

<sup>38</sup> Paul M. Schwartz & Daniel Solove, *Reconciling Personal Information in the United States and European Union*, 102 Calif. L. Rev. 877, 891 (2014) (emphasis in the original).



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Marshall Harlan Research Professor of Law at George Washington Law School.<sup>39</sup> The definition of personal information functions as an “on” switch for the application of information privacy law. Without the presence of personal information, the information privacy law regime generally does not apply. For example, **it is not customary to extend legal requirements to de-identified information.** As Professor Solove and I have written: “These laws share the same fundamental assumption—that in the absence of PII, there is no privacy right.”<sup>40</sup>

37. Moreover, a key challenge is that regulatory regimes sometimes treated identified and identifiable information the same. As Professor Solove and I wrote in a 2011 N.Y.U. Law Review article, **“whether information is identifiable to a person will depend upon context and cannot be determined *a priori*.”**<sup>41</sup>

*i. FTC Privacy Framework And Guidance.*

38. Before the FTC’s 2012 Report, there was a dearth of federal guidance on when data should be considered identifiable to an individual. The 2012 FTC guidance “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers” addressed this gap.<sup>42</sup> In the Staff Report, the Commission considered commenters’ concerns that,

---

<sup>39</sup> See *id.*; Paul M. Schwartz & Daniel J. Solove, *Defining “Personal Data” in the European Union and U.S.*, 13 Priv. & Sec. L. Rep. 1581 (Sept. 15, 2014); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814 (2011). For a comparative perspective on this issue, see Paul M. Schwartz, “*Personenbezogene Daten*” aus internationaler Perspektive, *Zeitschrift für Datenschutz* 97 (3/2011) (“Personal-specific Data” from an International Perspective).

<sup>40</sup> Schwartz & Solove, *Reconciling Personal Information in the United States and European Union*, *supra* note 34, at 879. See also, Paul M. Schwartz & Daniel J. Solove, *The PII Problem*, *supra* note 5, at 1877–83) (developing a model based on United States and EU law that frees aggregate data and “high-level information” from information privacy obligations).

<sup>41</sup> Schwartz & Solove, *The PII Problem*, *supra* note 5, at 1836.

<sup>42</sup> Federal Trade Commission (F.T.C.) Report, “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers” (March 26, 2012).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

with improvements in technology and the ubiquity of public information, more and more data could be “reasonably linked” to a consumer and that the proposed framework provided less incentive for a business to try to de-identify and prevent identification of the data it maintains. To address this challenge, the FTC Staff Report provided clarification to “give companies an incentive to collect and use data in a form that makes it less likely the data will be linked to a particular consumer or device, thereby promoting privacy.”<sup>43</sup> The FTC Staff clarified that data is not “reasonably linkable” to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.

39. According to the FTC Report, a company must take “reasonable measures” to ensure that the data is de-identified.<sup>44</sup> The FTC staff stated that, “[c]onsistent with the Commission’s approach in its data security cases, what qualifies as a reasonable level of justified confidence depends upon the particular circumstances, including the available methods and technologies.”<sup>45</sup> The FTC Staff subsequently also recommended “that the definition of PII only include information that is ‘reasonably’ linkable to an individual.”<sup>46</sup>

40. Additionally, the nature of data and the purposes for which it will be used are also relevant to a determination of whether data is de-identified. Thus, for example, whether or how a company publicly releases personal data affects whether the steps it has taken to de-identify data

---

<sup>43</sup> *Id.* at 22.

<sup>44</sup> *Id.* at 21.

<sup>45</sup> *Id.*

<sup>46</sup> In the Matter of Protecting the Privacy of Customers of Broadband & Other Telecommunications Services, WC Docket No. 16-106, Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission (May 27, 2016), <https://perma.cc/2EJZ-ENW8>.

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

are considered reasonable. Moreover, according to the FTC, there is no absolute standard for de-identification. Rather, companies are to take reasonable steps to ensure that data is de-identified. Depending on the circumstances, a variety of technical approaches to de-identification may be reasonable, such as deletion or obfuscation (*e.g.*, hashing) of data fields, the addition of sufficient “noise” to data, statistical sampling, or the use of aggregate or synthetic data.<sup>47</sup> In its 2012 Guidance, the Commission also encouraged companies and researchers to continue innovating in the development and evaluation of new and better approaches to de-identification.

41. Mr. Hochman’s approach is contrary to the FTC guidance because it fails to consider whether Google (1) takes reasonable measures to ensure that the Data at Issue is de-identified; (2) publicly commits not to try to re-identify the Data at Issue; and (3) contractually prohibits downstream recipients from trying to re-identify the Data at Issue.

*ii. ALI Data Privacy Principles.*

42. As noted above at Paragraph 10, the ALI was established in 1932 to promote the clarification and simplification of United States law and its adaptation to changing times. The ALI’s Data Privacy project began in 2012, and concluded with formal approval by ALI members at their annual meeting in 2019. Following final editorial work, the ALI published the Principles of Data Privacy Law in 2020.<sup>48</sup>

43. As also indicated above at Paragraph 10, I served as a co-reporter on the Data Privacy Principles project and am therefore familiar with it. It is important to note, however, that the Principles reflect the views of the entire ALI, and not merely my views and those of my co-reporter, Professor Solove. The Privacy Principles project constitutes the ALI’s judgment

---

<sup>47</sup> F.T.C. Report, “Protecting Consumer Privacy,” *supra* note 5, at 21.

<sup>48</sup> ALI Data Privacy Principles § 1 (Am. L. Inst. 2020).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

regarding U.S. information privacy standards. The Principles were created by an advisory group, the Members Consultative Group; the Council of the ALI; and the many ALI members who contributed to this project during its seven-year process. Moreover, as noted above, the ALI membership formally voted to approve the project, and did so by unanimous voice vote.

44. The ALI Data Privacy Principles contain concepts regarding responsibilities and obligations in the collection and use of personal data—ones that are in accordance with foundational elements of the U.S. approach to information privacy. The ALI Principles are designed to show the coherence of existing law and serve as a framework for industry-specific codes and data privacy model codes.<sup>49</sup> The ALI Principles set forth a series of responsibilities for those collecting or using personal data as well as a set of rights that individuals have regarding their personal information.

45. The ALI Data Privacy Principles define “personal data” as “any data that is identified or identifiable to a specific living individual.”<sup>50</sup> As the Principles state:

[I]t is impractical and undesirable to regulate data when the risk of identification is low. For example, personal data that has been properly de-identified and aggregated can be of great value to research and the advancement of knowledge. For that reason, the Data Privacy Principles are inapplicable to de-identified and aggregated data. When a low risk of identification exists, an application of the Data Privacy Principles would impose costs, burdens, and restrictions on the use of that data that far exceeded any benefit.<sup>51</sup>

46. Further, and according to the Data Privacy Principles, data is “identified” when “it is directly linked to a specific natural person, or when there is a *high probability* that it could be

---

<sup>49</sup> *Id.* at § 1, Introductory Note.

<sup>50</sup> *Id.* at § 2, Definitions (b).

<sup>51</sup> *Id.* § 2, Comment c.

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

linked to a specific person.”<sup>52</sup> Identified data is personal data under the Data Privacy Principles and is subject to all relevant ALI Principles.

47. Data is “identifiable” when “there is a *moderate probability* that [data] could be linked to a specific natural person by the intended recipient(s) or by others reasonably foreseeable to have access to the data.”<sup>53</sup> Under the Data Privacy Principles, identifiable data is subject to some of the ALI Principles but exempt from others.

48. Data is “nonidentifiable” when “there is a *low probability* that it could be linked to a specific natural person.”<sup>54</sup> Under the ALI Principles, such data is not personal data.<sup>55</sup>

49. The identifiability of data is not to be determined as an abstract or fixed matter. For example, computer scientists can develop new techniques to link personal data to specific individuals.<sup>56</sup> Accordingly, the ALI Data Privacy Principles propose that the identifiability of data is best viewed as a spectrum of high, moderate, and low categories relating to probabilities and actual practices, instead of black-or-white categories.<sup>57</sup>

50. Mr. Hochman’s bright-line, 29-bit definition of PII approach is inconsistent with these ALI principles because it fails to consider the probability that the specific Data at Issue could be linked to a specific natural person, or whether Google is taking specific steps to keep the Data at Issue from being linked to a specific natural person.

---

<sup>52</sup> *Id.* § 2, Definitions (b)(1) (emphasis added).

<sup>53</sup> *Id.* § 2, Definitions (b)(2) (emphasis added).

<sup>54</sup> *Id.* § 2, Definitions (b)(3) (emphasis added).

<sup>55</sup> *Id.*

<sup>56</sup> *Id.* § 2, Comment (c).

<sup>57</sup> *Id.*

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**iii. CCPA’s Definitions Of “Personal Information”.**

51. Mr. Hochman’s approach is fundamentally inconsistent with both definitions of PI used in the CCPA. By its terms, the CCPA limits its two definitions of “personal information” to the relevant portions of the statute. CCPA § 1798.140(v)(1) states that its definition of “[p]ersonal information” is made only “[f]or purposes of this title.” Similarly, CCPA § 1798.81.5(d)(1) defines “[p]ersonal information” only “[f]or purposes of this section.” Neither provision purports to define “personal information” for purposes of California law more broadly. Nor do these provisions purport to define the term “personal information” for purposes of interpreting the privacy policies of entities operating in California.

52. The first definition of PI in CCPA § 1798.140(o)(1)—which plaintiffs cite in their Complaint<sup>58</sup>—applies to the part of the CCPA that relies on actions by the California Attorney General for its enforcement,<sup>59</sup> and under which there is no private right of action for consumers. The California legislature considered—and rejected—a private right of action for any violation of

---

<sup>58</sup> TAC ¶ 155 (“the Data collected from users in “private browsing mode” qualifies as “personal information” that is protected by the CCPA. Cal. Civ. Code § 1798.140(o).”).

<sup>59</sup> Cal. Civ. Code § 1798.155(b) (“The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.”). As of July 1, 2023, a new regulatory authority, the California Privacy Protection Agency, will have authority to bring administrative actions to enforce certain provisions of the CCPA, and the California Attorney General’s Office will retain its authority to enforce the CCPA.

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

the CCPA.<sup>60</sup> Instead, the legislature cabined the private right of action to a narrow definition of personal information.<sup>61</sup>

53. The CCPA uses a second and separate definition of “personal information” (§ 1798.81.5(d)(1)) in a part of the statute that *does* provide a private right of action for consumers. The private right of action concerns the situation of a data breach. This section protects an individual “whose nonencrypted or nonredacted *personal information* ... is subject to an *unauthorized access* and exfiltration, *theft*, or *disclosure* as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action.”<sup>62</sup>

54. Where the CCPA provides a private right of action to consumers, that is, for certain cases of a data breach, it incorporates the definition of PI “as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5.”<sup>63</sup> For this part of the CCPA, “Personal information” means:

(A) An individual’s first name or first initial and the individual’s last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number. (ii) Driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account. (iv)

---

<sup>60</sup> In February 2019, California Attorney General Xavier Becerra and Senator Hannah-Beth Jackson introduced a proposed amendment to the CCPA that would have allowed consumers to bring a private right of action for any violation of the CCPA. *California Consumer Privacy Act of 2018: Consumer Remedies*, CA Sen. Bill. 561 (2019).

<sup>61</sup> See Christina H. Kroll, CCPA: The California Senate is Not Ready to Expand the Consumer Right of Action Proskauer Priv. L. Blog (May 17, 2019), <https://perma.cc/699Z-QENL>.

<sup>62</sup> Cal. Civ. Code § 1798.150(a)(1) (West 2018) (emphasis added).

<sup>63</sup> *Id.*

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Medical information. (v) Health insurance information. (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.<sup>64</sup>

Mr. Hochman fails to consider whether the Data at Issue in this case would be PI under this CCPA definition. According to Mr. Hochman’s descriptions of the Data at Issue in this case,<sup>65</sup> however, it appears that none of it falls under this CCPA definition of PI. The Data at Issue is URLs, IPs, and cookies not associated with a Google Account. None of this information is PI under this definition of the CCPA.

55. Mr. Hochman’s approach is also contrary to the first definition of PI in the CCPA:

Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.<sup>66</sup>

The statute then enumerates categories of information that are PI if they are reasonably capable of being linked to a particular consumer, including:

- “(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.”<sup>67</sup>
- “(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an internet website, application, or advertisement.”<sup>68</sup>

---

<sup>64</sup> Cal. Civ. Code § 1798.81.5(d)(1) (West 2018).

<sup>65</sup> Hochman ¶ 99 (“URLs, IP addresses, user agent, referer”).

<sup>66</sup> Cal. Civ. Code § 1798.140(o)(1).

<sup>67</sup> *Id.*

<sup>68</sup> *Id.*



## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

56. The plain language establishes that an “online identifier,” “internet protocol address,” “browsing history,” or “search history” are “personal information” under this section of the CCPA only if they can be *reasonably linked* to a particular consumer or household. But, if a particular “online identifier,” “internet protocol address,” “browsing history,” and “search history” cannot be reasonably linked to a particular consumer or household then it is not “personal information.” Here, too, the CCPA follows the same approach we see in the other information privacy standards surveyed, namely, the FTC Privacy Framework and Guidance and the ALI Data Privacy Principles.

57. In addition, the CCPA does not apply to and expressly excludes “deidentified” information from the scope of its coverage.<sup>69</sup> The CCPA defines the term with care in Section 1798.140(h): “‘Deidentified’ means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a *particular consumer*, provided that a business that uses deidentified information:

- (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
- (2) Has implemented business processes that specifically prohibit reidentification of the information.
- (3) Has implemented business processes to prevent inadvertent release of deidentified information.
- (4) Makes no attempt to reidentify the information.”

58. Moreover, the CCPA provides a means for a business, such as Google, to process data in a manner that results in it no longer being linked to a particular consumer or household.

---

<sup>69</sup> Cal. Civ. Code § 1798.145(a) (“The obligations imposed on businesses by this title shall not restrict a business’ ability to...(5)[c]ollect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.”); Cal. Civ. Code, §1798.140(o)(3) (“Personal information” does not include consumer information that is deidentified or aggregate consumer information.”).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

The CCPA defines “pseudonymize” or “pseudonymization” as “the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.”<sup>70</sup> Therefore, even if specific information could reasonably be linked to an individual when a business first receives it, the CCPA provides a path under which a business can process data to prevent it from being linked to a particular consumer.

59. Thus, the CCPA’s definition of “personal information” considers whether data is reasonably linkable (or whether it has undergone pseudonymization) and how a business processes data. Mr. Hochman’s theory is inconsistent with the CCPA’s definition of “personal information.”

60. The California Privacy Rights Act (CPRA), also known as Proposition 24 (and sometimes referred to as CCPA 2.0), is a ballot measure that was approved by California voters on November 3, 2020. The CPRA amends the provisions of the CCPA of 2018. While the CPRA took effect on December 16, 2020, most of the provisions revising the CCPA only become “operative” on January 1, 2023.

61. There are two pertinent CPRA amendments in relation to personal information in the context of these reports. *First*, the CPRA narrows a wide range of the obligations imposed on businesses by making clear that they “shall not apply to Household data.”<sup>71</sup> These narrowed obligations are found in the following sections: 1798.105 (consumers’ rights to delete personal information), 1798.106 (consumers’ rights to correct inaccurate personal information), 1798.110

---

<sup>70</sup> Cal. Civ. Code § 1798.140(r).

<sup>71</sup> Cal. Civ. Code § 1798.145(p).

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

(consumers’ right to know what personal information is being collected), and 1798.115 (consumers’ right to know what personal information is sold or shared and to whom).

62. *Second*, the CPRA seeks to encourage businesses to keep information in the least or in a lesser identifiable form. It incentivizes such behavior by freeing these enterprises from certain obligations. In pertinent part, it states, “[t]his title shall not be construed to require a business, service provider, or contractor to:

(1) Reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(2) Retain any personal information about a consumer if, in the ordinary course of business that information about the consumer would not be retained.

(3) Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.<sup>72</sup>

If companies maintain non-PII, for example, the CPRA exempts them from reidentifying such information, or retaining it, or keeping it in a fashion that will allow it to be used to respond to an individual’s request to access their information.

63. Mr. Hochman does not take these CPRA amendments into consideration. This gap in his opinion further indicates that his opinions are contrary to U.S. privacy standards.

**V. Opinion # 2: Mr. Schneier’s Opinions On PI, PII, And Identifying Information Are Similarly Defective And Also Suffer From Additional Deficiencies Due To An Over-Inclusive Framework Where Virtually Any Data Can Be Deemed PII.**

64. For the reasons stated above, Mr. Schneier’s report suffers from the same deficiencies as Mr. Hochman’s report, including (i) a failure to draw on U.S. information standards governing PII, PI, and identifying information; (ii) an absence of acknowledgment that business practices, policies and procedures affect the categorization of information that is identifying and

---

<sup>72</sup> Cal. Civ. Code § 1798.145(j).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

non-identifying. In addition, Mr. Schneier’s report suffers from additional shortcomings resulting from his broad and amorphous conception of PI and PII, which would result in a vastly over-inclusive and impractical privacy framework.

65. In contrast to Mr. Hochman, Mr. Schneier offers a broader definition of PI that, according to him, “focus[es] not only on how information is used but how information could be used (*e.g.*, ‘can be used,’ ‘could reasonably be linked’).”<sup>73</sup> In considering how information could be used, however, Mr. Schneier does not look at actual Google practices that are in place to restrict its abilities and possibilities to link data. Mr. Schneier cites to one of the California Consumer Privacy Act’s definitions of “personal information” and states that such definition is consistent “with [his] understanding as a technologist and with common usage in the field of privacy and security”:

[I]nformation that identifies, relates to, or ***could reasonably be linked with you*** or your household. For example, it could include your name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.<sup>74</sup>

66. As explained above, (i) the CCPA’s concept of “could reasonably be linked” calls for contextual analysis that includes an examination of a company’s practices and policies; and (ii) the CCPA recognizes important categories of de-identified data and pseudonymous data.

67. In an effort to suggest it is not possible to maintain a distinction between PII and non-PII, Mr. Schneier cites to the Code of Federal Regulations definition of PII:

[I]nformation that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and

---

<sup>73</sup> Schneier ¶ 82.

<sup>74</sup> Schneier ¶ 81 (emphasis added).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. [...] *[N]on-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available [non-PII] information, could be used to identify an individual.*<sup>75</sup>

In this part of his opinion, Mr. Schneier cites a definition of PII that comes from Title 2 of the CFR and specifically refers to “Grants and Agreements,” a topic unrelated to the issue here. In fact, PII is only referenced once in Title 2 and only in the context of restrictions on public access to records.<sup>76</sup>

No Federal awarding agency may place restrictions on the non-Federal entity that limit public access to the records of the non-Federal entity pertinent to a Federal award, except for protected **personally identifiable information (PII)** or when the Federal awarding agency can demonstrate that such records will be kept confidential and would have been exempted from disclosure pursuant to the Freedom of Information Act (5 U.S.C. 552) or controlled unclassified information pursuant to Executive Order 13556 if the records had belonged to the Federal awarding agency.<sup>77</sup>

68. Even the website Mr. Schneier used, which allows individuals to click on the term PII through the applicable language in 2 CFR § 200.338, states:

These are the definitions for terms used in this part. **Different definitions may be found in Federal statutes or regulations that apply more specifically to particular programs or activities.** These definitions could be supplemented by additional instructional information provided in government wide standard information collections. For purposes of this part, the following definitions apply[.]<sup>78</sup>

---

<sup>75</sup> Schneier ¶ 80 citing 2 CFR § 200.79.

<sup>76</sup> 2 CFR § 200.79, <https://perma.cc/P9HC-XF2U>.

<sup>77</sup> 2 CFR § 200.338, (emphasis added) <https://perma.cc/8E4S-2XMY>.

<sup>78</sup> 2 CFR § 200.1 (emphasis added) (limiting the scope of 2 CFR § 200.338), <https://perma.cc/U9C2-UVVL>.

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

69. In his report, Mr. Schneier treats “identifying information” in a sweeping and tautological fashion as information that identifies individual users. For example, Mr. Schneier writes that “records purportedly stripped of *identifying information* could nonetheless be combined with other data in a manner that enabled patients to be personally identified.”<sup>79</sup>

70. At a high level, Mr. Schneier offers a totalizing theory in which data is never truly de-identified because it can always be re-identified. This methodology is contrary to U.S. information privacy standards which (a) recognize that data can be de-identified, and (b) place anonymous data outside its scope of protections.

71. Mr. Schneier further states:

And even if Google is not building user profiles across signed-in and signed-out data, Google’s decision to collect and log this data creates the potential for data to be joined in this way. For example, Google’s storage of unique identifiers and IP addresses together in logs introduces a risk that data from a users’ private browsing will be joined with a user’s signed-in data.<sup>80</sup>

This statement is one example of Mr. Schneier being at odds with U.S. information privacy standards, which consider the probability that data will be linked to an individual.

72. In particular, it is essential under these standards to consider policies and practices that Google has adopted to limit its capabilities and latitude to link information.

73. Indeed, Mr. Schneier’s approach would have grave implications for these information privacy standards. By considering theoretical and abstract possibilities sufficient to make data into PII, Mr. Schneier would move these standards beyond their current concept of PII. His approach would undercut the current means of establishing coherent boundaries on necessary

---

<sup>79</sup> Schneier ¶ 224 (emphasis added).

<sup>80</sup> Schneier ¶ 205.

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

regulation.<sup>81</sup> As a concept, PII helps to set limits on the scope of privacy law.<sup>82</sup> As Daniel Solove and I have written, “In a world overflowing with information, the law cannot possibly regulate all of it.”<sup>83</sup>

74. The risk of having too broad or too abstract a definition of PII is to permit an expansion of regulation to a nearly infinite array of information, including practically every piece of statistical or demographic data.<sup>84</sup> Such an expansion would be highly problematic. To again reference my work with Daniel Solove, a concept of PII that looks to the context of data use has a number of positive benefits. First, by drawing a line between PII and non-PII, it permits society to reap the benefits of large data sets, which “play an important role in research, health care, data security, and the dissemination of knowledge generally.”<sup>85</sup> Second, drawing a line between PII and non-PII based on the practices of a data processing entity creates an incentive for collecting and maintaining information in the least identifiable form. As Professor Solove and I argue, it can encourage companies to “invest in technologies that truly make identification of personal data less likely.”<sup>86</sup> Finally, by looking to the context of data use, one promotes privacy by incentivizing the use of non-PII. Consider a regulatory system that required full access rights for individuals even for de-identified data that a company had pledged to maintain as non-PII, or when there was a theoretical, low probability of re-identification of non-PII. In requiring that this information be

---

<sup>81</sup> Paul M. Schwartz & Daniel J. Solove *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814, 1836–1848 (2011).

<sup>82</sup> *Id.* at 1866.

<sup>83</sup> *Id.*

<sup>84</sup> *Id.*

<sup>85</sup> *Id.*

<sup>86</sup> *Id.* at 1887.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

maintained so it would always be transformable into PII, the critical privacy principle of minimization of personal data would be undercut.

**VI. Opinion # 3: Mr. Hochman And Mr. Schneier Have Classified The Data At Issue Incorrectly.**

75. In this section, I evaluate the Data at Issue using the frameworks that Mr. Hochman and Mr. Schneier have set forth; the U.S. information privacy standards expressed in (A) the FTC Guidance (B) the ALI Principles and (C) the CCPA; and (D) Google policies and practices. *See supra* § IV.B. In my opinion, the conclusions that Mr. Hochman and Mr. Schneier reach that the Data at Issue is PI, PII, or identifying information is fundamentally flawed. Had they applied the correct analysis based on governing U.S. privacy standards and Google policies and procedures, they would have been obliged to conclude that the Data at Issue is not personally identifying; that there is a low probability of Google’s identification of users; and that the Data at Issue is likely to be exempt from data subject access rights under current U.S. information privacy standards.

**A. Mr. Hochman And Mr. Schneier Fail To Take Into Account Google’s Policies And Procedures Related To Classifying The Data At Issue.**

76. For technical descriptions of the Data at Issue, I am relying on the report of computer scientist Dr. Konstantinos Psounis, and in particular his opinion that the Data at Issue is not associated with a user’s Google Account and the Data at Issue is stored in an orphaned and unidentified state.<sup>87</sup>

77. An analysis of Google’s policies and guidelines demonstrates the presence of strong privacy protections designed to prevent such Data at Issue from being identified and linked to a particular consumer, or a user’s Google Account. Neither Mr. Hochman’s categorical approach nor Mr. Schneier’s amorphous and open-ended framework take into account Google’s policies and

---

<sup>87</sup> Expert Report of Konstantinos Psounis, PH.D. § III.A.1-2.



## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

guidelines regarding data. Their perspectives are faulty because, as explained above, the steps a company takes to process data to prevent it from being reasonably linked to an identified individual are a key factor in determining its status under relevant information privacy standards. In my opinion, Google's existing policies and guidelines support the conclusion that the Data at Issue is neither PII nor PI. Mr. Hochman does not establish that Google links the Data at Issue with a Google Account; rather, he merely speculates that Google *could* join the Data at Issue with an individual's Google Account. He also does not consider the *likelihood* that this would ever occur and the existence of Google safeguard to prevent such joining of data.

78. In this section, I respond to Mr. Hochman's and Mr. Schneier's Expert Opinions by examining Google's relevant policies. Google has implemented policies and taken certain steps regarding the Data at Issue, namely information that is *not* associated with a user's Google Account. These steps seek to ensure that such information is neither linked nor reasonably linkable to a specific individual by Google. Moreover, Google's Anti-Fingerprinting Policy prevents certain steps by Google employees that might increase the identifiability of certain information. These policies are described more fully in the sections that follow.

79. The information privacy standards that this Expert Opinion examined above, namely the ALI Data Privacy Principles, the FTC Staff Report, and the CCPA, underscore the relevance of Google's policies and practices. Specifically, these standards require consideration of what companies permit and do not permit with personal data. As a consequence, Google's Privacy Policy, Data Categorization Guidelines, and Anti-Fingerprinting policy are highly significant documents for classifying the Data at Issue.

80. To be clear, I am not analyzing whether it is theoretically possible for Google, or a rogue Google employee, to identify an individual using non-Google Account linked data through

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

“finger-printing.” Whether data is “theoretically linkable” to an individual is not a standard for determining whether data is PI or PII. Moreover, my understanding is that “finger-printing” would be in violation of Google’s policies and also would require circumvention of Google’s technical barriers that apply to the segregated repositories that Google uses to store data.

*i. Google’s Privacy Policy.*

81. The Google Privacy Policy defines “personal information” as “information that you provide to us which personally identifies you, such as your *name, email address, or billing information*, or other data that can be *reasonably linked to such information by Google*, such as information *we associate with your Google Account*.”<sup>88</sup> Under this definition, apart from enumerated categories of information that personally identify an individual—*i.e.* name, email address, billing information—data is “personal information” only if Google can reasonably link it to an identified individual. Thus, plaintiffs’ categorical approach of defining PI as *always* including the Data at Issue is inconsistent with Google’s own Privacy Policy definition. Under that definition of “personal information,” the Data at Issue *does* fall in this category when Google associates it with the user’s Google Account.

82. When Google does not associate the Data at Issue with a user’s Google Account, and takes steps to ensure the data cannot reasonably be linked to information that personally identifies an individual—*e.g.*, when Google implements protocols and policies to prevent such linking—as is the case here, the Data at Issue is not “personal information” under the Google Privacy Policy. Whether, when, and which data is reasonably linkable by Google to information

---

<sup>88</sup> Google Privacy & Terms, Privacy Policy Key Terms (Last Accessed Jun. 3, 2022), <https://perma.cc/524M-5UH2> (emphases added).

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

that personally identifies an individual depends on Google’s practices and policies (namely, those discussed in the three sections that follow).

*ii. Google’s Data Categorization Guidelines.*

83. Beyond the Google Privacy Policy, another important privacy instrument in use at Google is its Data Categorization Guidelines.<sup>89</sup> This document defines “User Data” as [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>90</sup> The Google Data Categorization Guidelines further state, [REDACTED]

[REDACTED]

[REDACTED]<sup>91</sup> These Google Guidelines define them as follows:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

<sup>89</sup> Data Categorization Guidelines, GOOG-CABR-04400013.

<sup>90</sup> *Id.*

<sup>91</sup> *Id.* at -014.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

[REDACTED]

[REDACTED]

84. Google Guidelines also state, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>93</sup>

85. Google's Data Categorization Guidelines applies the following basic guidelines to categorizing data as identifiable/PII:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

<sup>92</sup> *Id.* at -014-15.

<sup>93</sup> *Id.* at -015 (emphasis added).

<sup>94</sup> *Id.* at -014.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

86. In my opinion, Google’s data categorization guidelines reflect the U.S. information privacy standards discussed in this report. An important aspect of how these guidelines incorporate these standards is their incorporation of a benchmark of whether data is “reasonably likely” to identify any person.

**iii. Google’s Anti-Fingerprinting Policy.**

87. Since January 2015, Google has maintained an official Internal Privacy Policy on the use of device/app/browser fingerprinting and immutable identifiers.<sup>95</sup> Google’s anti-fingerprinting policy prohibits the use of [REDACTED]

[REDACTED] As a consequence of this anti-fingerprinting policy, Google employees are prohibited from using specific categories of the Data at Issue—*i.e.*, IP address, User-Agent, X-Client-Data Header<sup>97</sup>—to identify and track a browser or user across distinct transactions.

88. Google’s platform policies make explicitly clear that Google’s platform products—which include “Authorized Buyers, Campaign Manager 360, Google Ad Manager 360, Google Ad

---

<sup>95</sup> See Device/App/Browser Fingerprinting and Immutable Identifiers Policy, GOOG-CALH-00027147.

<sup>96</sup> *Id.* (Google’s anti-fingerprinting policy explicitly lists “IP address” as an example of an attribute that should be considered unique).

<sup>97</sup> Decl. of Alexei Svitkine ¶ 4, Dkt. 112-5 (“The X-Client-Data header is designed to have low entropy and is not uniquely identifying. Indeed, the header assigned to a particular instance of Chrome is based on a random number from 0 to 7999 precisely to prevent it from being used to uniquely identify the user or browser. In practical terms, this means that the XClient-Data header for any particular instance of Chrome is identical to the header assigned to many other Chrome users.”).

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Manager, Search Ads 360, and Display & Video 360”<sup>98</sup>—must not be used “to identify users or facilitate the merging of personally-identifiable information with information previously collected as non-personally identifiable information without robust notice of, and the user’s prior affirmative (*i.e.* opt-in) consent to, that identification or merger.”<sup>99</sup> Irrespective of users’ consent, there must be no attempt to disaggregate data that Google reports in aggregate.<sup>100</sup> Furthermore, to “protect user privacy, Google policies mandate that no data be passed to Google [by Google Analytics customers] that Google could use or recognize as personally identifiable information (PII).”<sup>101</sup>

89. Google’s anti-fingerprinting policy is a function of its strong policy against anti-fingerprinting. Google has publicly stated that “Google doesn’t use fingerprinting for ads personalization because it doesn’t allow reasonable user control and transparency. Nor do we let others bring fingerprinting data into our advertising products.”<sup>102</sup> Google has publicly confirmed it will “continue to disallow fingerprinting on its products and via its platforms, as per its long-standing policies.”<sup>103</sup>

90. Therefore, in the context of fingerprinting, Google has a stated policy that expressly prohibits the use of certain of the Data at Issue to identify users. Moreover, Google publicly commits to not using the Data at Issue to identify users. Finally, Google contractually prohibits

---

<sup>98</sup> *Platforms Program Policies*, Google Help Center, (Last Updated Apr. 1, 2022), <https://perma.cc/7D86-XR54>.

<sup>99</sup> *Id.*

<sup>100</sup> *Id.*

<sup>101</sup> Best Practices to Avoid Sending Personally Identifiable Information (PII), Analytics Help Center, (2021), <https://perma.cc/L7LG-CG7W>.

<sup>102</sup> Prabhakar Raghavan, Raising the Bar on Transparency, Choice and Control in Digital Advertising, (May 7, 2019), Google Ads & Commerce Blog, <https://perma.cc/HQH3-PPBE>; *see also* GOOG-CALH-00029480.

<sup>103</sup> GBO Comms Document, GOOG-CABR-04310004.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

other companies from identifying users as well. All of these factors must be taken into consideration when classifying the Data at Issue.

*iv. Google's Policies Against Re-Identifying Individuals.*

91. Google's Log Data Usage Rules contain a series of prohibitions for Google employees that bear directly on Mr. Hochman's Expert Opinions. Specifically, Google's User Data Anonymization Policy prohibits Google employees from re-identifying any individual from Anonymous or Pseudonymous data.<sup>104</sup> [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>107</sup>

92. Google's 2020 Log Data Usage Rules include a relevant section on re-identification of logs data.<sup>108</sup> I have reproduced it here:

---

<sup>104</sup> Log Data Usage Rules, GOOG-BRWN-00029004 at -006.

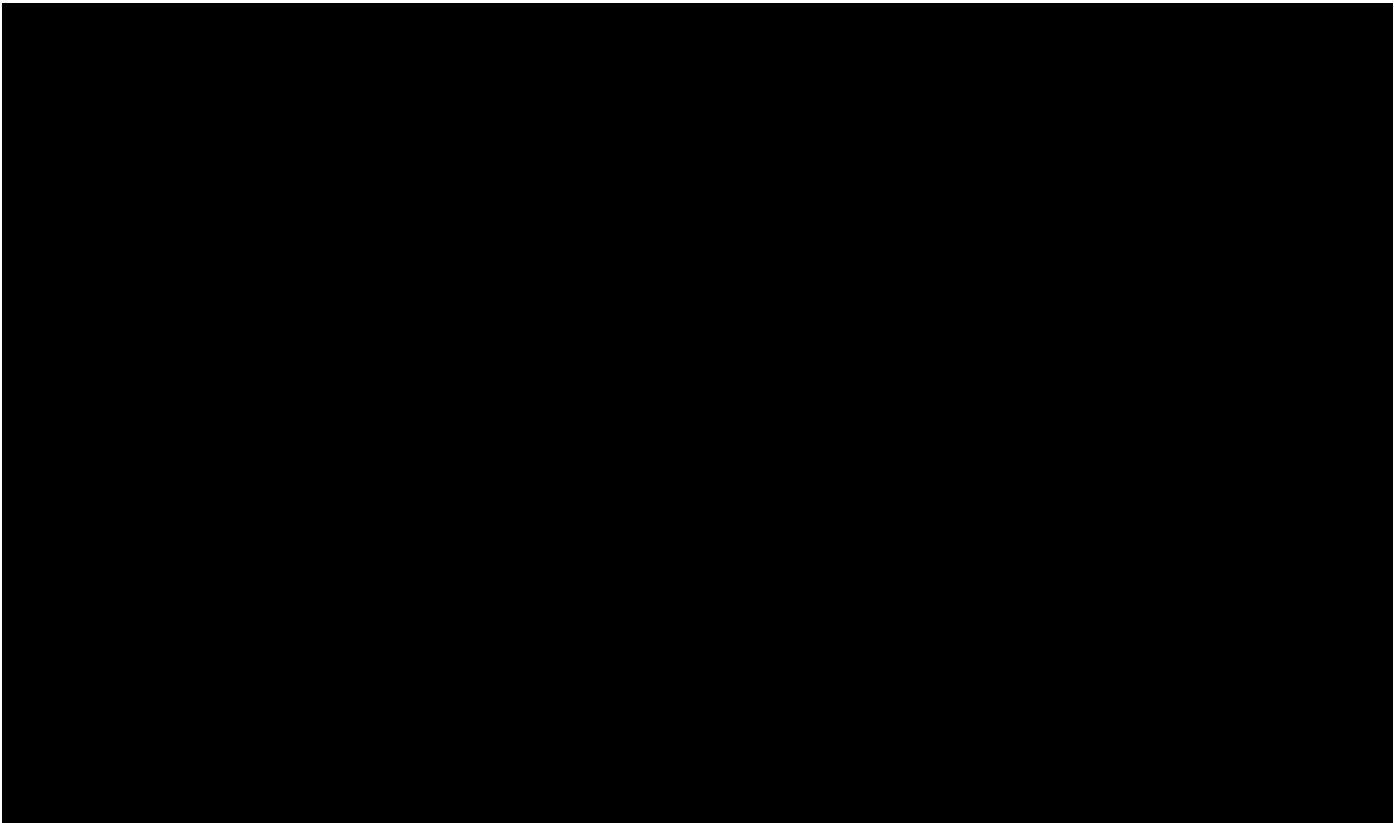
<sup>105</sup> *Id.*

<sup>106</sup> *Id.*

<sup>107</sup> *Id.* See also Google Factbase: Ads Data Policies and Statements, GOOG-CABR-0460448

<sup>108</sup> See GOOG-BRWN-00029004; see also Monsees Dep. (30b6) at 311:12-313:12, Apr. 9, 2021, *Calhoun v. Google*, 5:20-cv-05146-LHK.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER



GOOG-BRWN-00029004 at -006.

93. In addition, as Google employee David Monsees explained in a declaration filed in the *Calhoun v. Google* action, Google engages in the following practices to ensure that pseudonymous-keyed log data are not used to uniquely identify individual users including: IP address redaction and cookie scrubbing,<sup>109</sup> limiting the access of individual Googlers to either pseudonymous-keyed data sources or Google Account-keyed data sources,<sup>110</sup> prohibiting determinative joins between Google Account-keyed data and pseudonymous-keyed data,<sup>111</sup> avoiding logging specific IDs to prevent an indirect and inadvertent join between Google Account-keyed data and pseudonymous-keyed data,<sup>112</sup> and ensuring that “identifiers such as Biscotti or

---

<sup>109</sup> Scrubbing Policies for Log Data, GOOG-CALH-00027152.

<sup>110</sup> Ads Cookies, GOOG-CABR-04696282 at -284.

<sup>111</sup> *Id.* at -285.

<sup>112</sup> *Id.*



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

Zwieback must never be stored with personally-identifying information (PII) such as GAIA IDs [Google Account IDs].”<sup>113</sup>

**B. The Data At Issue Is Not Personally Identifying, Has A Low Probability Of Identification, And Is Exempt From Data Subject Access Rights.**

***i. The Data At Issue Is Not Reasonably Linkable Under FTC Guidance.***

94. Both Mr. Hochman and Mr. Schneier fail to consider what qualifies as “reasonably linkable” data under the FTC and what Google does in practice in relation to this FTC guidance. As illustrated in the table below, my analysis of Google’s relevant policies and practices shows that Google takes steps to make the Data at Issue not “reasonably linkable” pursuant to the FTC guidance.

#	FTC Guidance Data is not “reasonably linkable” to the extent that a company:	Google Policies and Practices
1.	“Takes reasonable measures to ensure that the data is de-identified;”	[REDACTED]
2.	“[P]ublicly commits not to try to re-identify the data; and”	<ul style="list-style-type: none"> <li>• “Chrome also announced that it will more aggressively restrict</li> </ul>

<sup>113</sup> *Id.* at -286. *See also*, Decl. of D. Monsees ¶10, Calhoun v. Google, 5:20-cv-05146-LHK, (Dkt. No. 428-22).

<sup>114</sup> *See supra* § VI.A.iv.

<sup>115</sup> *Id.*

<sup>116</sup> *Id.*

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

		<p>fingerprinting across the web.”<sup>117</sup></p> <ul style="list-style-type: none"> <li>• “[We] will aggressively combat the current techniques for non-cookie based cross-site tracking, such as fingerprinting, cache inspection, link decoration, network tracking and Personally Identifying Information (PII) joins.”<sup>118</sup></li> <li>• “[W]e’re developing techniques to detect and mitigate covert tracking and workarounds by launching new anti-fingerprinting measures to discourage these kinds of deceptive and intrusive techniques.”<sup>119</sup></li> <li>• “Google doesn’t use fingerprinting for ads personalization because it doesn’t allow reasonable user control and transparency.”<sup>120</sup></li> </ul>
3.	“contractually prohibits downstream recipients from trying to re-identify the data.”	<ul style="list-style-type: none"> <li>• “Nor do we let others bring fingerprinting data into our advertising products.”<sup>121</sup></li> <li>• “You must not use device fingerprints or locally shared objects (e.g., Flash cookies, Browser Helper Objects, HTML5 local storage) other than HTTP cookies, or user-resettable device identifiers designed for use in measurement or advertising, in connection with Google Analytics.”<sup>122</sup></li> <li>• “[W]e remind you that our policies prohibit fingerprinting for identification (e.g., Requirements for Third Party Ad Serving), and we require that you adhere to our policies, which can be more restrictive than the TCF v2.0 in some cases, whenever you work with us.”<sup>123</sup></li> <li>• “Ads may not directly capture any personally-identifiable user information. Personal information includes, but isn’t limited to, e-mail addresses, telephone numbers, and credit card numbers.</li> </ul>

<sup>117</sup> Prabhakar Raghavan, Raising the Bar on Transparency, Choice and Control in Digital Advertising, (May 7, 2019), Google Ads & Commerce Blog, <https://perma.cc/HQH3-PPBE>.

<sup>118</sup> *The Privacy Sandbox*, Chromium Blog, <https://perma.cc/7GGQ-7YV7> (last accessed Jun. 4, 2022).

<sup>119</sup> Justin Schuh, *Building a more private web: A path towards making third party cookies obsolete*, Chromium Blog, (Jan. 14, 2020), <https://perma.cc/8LCF-7N4A>.

<sup>120</sup> Prabhakar Raghavan, Raising the Bar on Transparency, Choice and Control in Digital Advertising, (May 7, 2019), Google Ads & Commerce Blog, <https://perma.cc/HQH3-PPBE>.

<sup>121</sup> *Id.*

<sup>122</sup> *Policy Against Fingerprints and Locally Shared Objects*, Google Analytics Help Center (2022), <https://perma.cc/V44X-GEZK>.

<sup>123</sup> *Interoperability guidance for vendors working with Google via the IAB TCFv2.0*, Google Ad Manager Help Center (2022), <https://perma.cc/EC8S-MVJK>.

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

		<p>No sensitive information can be collected through the ad.</p> <p>You may not associate cookies, web beacons, or other tracking mechanisms with personally-identifiable information (PII) for any purpose or with precise user location for behavior targeting unless the user has knowingly and expressly opted in. (For purposes of this document, PII and precise user location does not include IP addresses.)”<sup>124</sup></p>
--	--	---

95. Based on comparing Google’s practices with its publicly available policies and procedures, it is my opinion that Google, as recommended by the FTC, “[t]akes reasonable measures to ensure that the data is de-identified; publicly commits not to try to re-identify the data; and contractually prohibits downstream recipients from trying to re-identify the data.”

***ii. Under ALI Principles, There Is A Low Probability That Google Could Link The Data At Issue To A Specific Natural Person.***

96. Under the ALI Data Privacy Principles, data is “identified” when “it is directly linked to a specific natural person, or when there is a *high probability* that it could be linked to a specific person.”<sup>125</sup> It also explains that data is ““nonidentifiable”” when there is a low probability that it could be linked in to a specific natural person.”<sup>126</sup> Such information is not “personal data” under the Data Privacy Principles.<sup>127</sup> Indeed, the Principles establish the idea of “spectrum of probabilities” for defining personal data.<sup>128</sup> As indicated above, both Mr. Hochman and Mr. Schneier fail to adequately consider Google’s privacy policies and practices. Due to these policies

<sup>124</sup> *Requirements for third-party ad serving*, Google Advertising Policies Help (2022), <https://perma.cc/JP2W-8H7Z>.

<sup>125</sup> ALI Data Privacy Principles § 2, Definitions (b)(1) (emphasis added).

<sup>126</sup> *Id.* at (b)(3).

<sup>127</sup> *Id.*

<sup>128</sup> *Id.* at Comment (c).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

and practices, there is not a “high probability” that the Data at Issue can be linked to a specific person. Rather, as a result of Google’s privacy policies and practices, there is a low probability that the Data at Issue is personal data that is not directly linked to a specific natural person.

**iii. *The Data At Issue Is Exempt From Certain Breach Notification Requirements, Portability, and Access and Correction Rights.***

97. As in defining “personal data,” the ALI Data Privacy Principles rely on a contextual approach when it discusses the requirement for data breach notifications. The Principles free data processors from any obligations to notify an affected party of such breaches under circumstances when there is “a low probability” of risk. It states:

(5) The factors to be considered in determining whether there is a *low probability* that personal data will be compromised include:

- (A) the nature and extent of the personal data involved, including the types of identifiers and the likelihood of reidentification;
- (B) the identity of the unauthorized person to whom the personal data was disclosed or who used it;
- (C) whether the personal data was actually acquired or accessed; and
- (D) the extent to which the risk of compromise of the personal data has been mitigated.

(6) Notification is not required when the personal data was properly encrypted and the encryption keys are not compromised or breached.<sup>129</sup>

98. Crucially, this language indicates that even when personal data is involved in a breach, a critical requirement continues to be a contextual analysis, and one that turns on an evaluation of risk factors.

99. As for a data portability request, it “permits a data subject to control his or her *personal information* and can also further consumer choice among enterprises.”<sup>130</sup> The idea of

---

<sup>129</sup> ALI Data Privacy Principles, § 11 Data Security and Data Breach Notification. (emphasis added).

<sup>130</sup> ALI Data Privacy Principles, § 9 Data Portability, Comment (a).

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

data portability is to allow consumers to request and receive the personal data that one company has collected about them, and then be able to move the data to another company. Importantly, pursuant to ALI Principles, “[i]f only identifiable personal data is maintained about a data subject and if complying with a data portability request would require identifying this personal data, then the data controller **does not have to comply with the data portability request.**”<sup>131</sup> Thus, the Data at Issue is exempt from data subject portability interests as defined in the ALI Data Privacy Principles.

100. Finally, there is the matter of access and correction rights. The ALI Principles allow individuals to access their personal data and request corrections of errors. These interests are limited, however, only to identified data. Indeed, the ALI Data Privacy Principles explicitly state, “[a]ccess and correction rights extend under these Principles only to identified data and not identifiable data.”<sup>132</sup> Recall that “identifiable data” is information where there is a moderate probability of linkage to a specific person, but that connection has not yet been made. The Principles warn:

Access and correction rights do not extend to identifiable data because such rights would result in more personal data becoming identified, which would increase risks to the privacy and security of data. Such an interest might also impose excessive compliance costs on data controllers, who would be obligated to carry out onerous searches of their databases for information that was linkable to a specific individual.<sup>133</sup>

The Data at Issue provides a clear illustration of information that is not identified, and, hence, not subject to access and correction interests pursuant to the ALI Data Privacy Principles.

---

<sup>131</sup> *Id.* at § 9(f), Data Portability (emphasis added).

<sup>132</sup> *Id.* at § 8, Comment b.

<sup>133</sup> *Id.*

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

**C. Individualized Determinations Would Be Required In Any Attempt To Establish That The Data At Issue Is PI Or PII.**

101. In my opinion, as stated above, the Data at Issue is non-identifying and not PII or PI under U.S. privacy industry standards. Any attempt to show otherwise would necessarily require fact-intensive and individualized inquiries for each Data at Issue and each putative class member. That result follows because whether the Data at Issue has any probability of being reasonably likely to identify a particular class member cannot be uniformly answered as to all class members as the class is currently defined.<sup>134</sup> Such a determination is necessarily a fact-bound one that will turn on the type of data; whether the specific data is pseudonymous or anonymous; and whether Google has processed the specific data to de-identify, pseudonymize, or prevent individual identification.

102. The easiest scenario under which data is likely PI or PII is one that does not apply to this case. Under this scenario Google associates certain data (IP address, user-agent, cookies, and URLs) with a user's Google Account. In that scenario, the Data can be classified as PI under most standards.<sup>135</sup> Specifically, such data is likely to be "identified" information under the ALI Data Privacy principles; it is likely PI under the FTC Guidance; and it is likely PI under one provision of the CCPA, namely § 1798.140(o)(1).

103. However, as demonstrated above, Google does not associate the Data at Issue with a user's Google Account. Hence, the determination of whether the data related to a putative class member's browsing is PI or PII necessarily raises a series of complex factual questions. Under the FTC guidance, a determination has to be made on whether the data is "reasonably linkable" to a

---

<sup>134</sup> TAC ¶ 192. *See also*, TAC ¶ 93 .

<sup>135</sup> I discuss Google's Privacy Policy above in this Expert Opinion. *See supra* § VI.A.i.

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

consumer or their device.<sup>136</sup> Under the ALI principles, the probability that such data is linked to an identified individual has to be taken into consideration.<sup>137</sup> Similarly, under the CCPA section that plaintiffs cite in their Complaint and Mr. Schneier references (1798.140(o)(1)), data is PI if it could reasonably be linked with a particular consumer.<sup>138</sup> Under either of these approaches, whether Data at Issue is non-identifying or has a low probability of identification requires additional individualized fact-intensive determinations for each individual set of data and cannot be made on a classwide basis.

104. To illustrate the above, I briefly discuss two of the types of Data at Issue in this case below.

- (a) **IP Address.** The degree to which any given IP address is non-identifying or has a low probability of identification varies and will turn on answers to a number of questions, including: Is the IP address cloaked through a VPN? Is the IP address associated with an individual's home address or is it associated with a place generally open to the public? The latter kind of a location would include a coffee shop that offers wifi, such as a Starbucks. Other issues are relevant to the issue of judging whether an IP address is "personal information." Is the IP address static or

---

<sup>136</sup> Federal Trade Commission (F.T.C.), Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, at 22 (March 26, 2012).

<sup>137</sup> ALI Data Privacy Principles § 2, Comment c.

<sup>138</sup> *See also*, "The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 shall not apply to household data." Cal. Civ. Code § 1798.145(p), *AB-2891 California Consumer Privacy Act: exemption*. AB-2891 or the California Privacy Rights Act (CPRA) is a ballot measure (Proposition 24) that was approved by California voters on November 3, 2020 and took effect on December 16, 2020; however, most of the provisions revising the CCPA will become operative by January 1, 2023. The CPRA significantly amends the CCPA, and it is periodically referred to as "CCPA 2.0."

## CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

dynamic?<sup>139</sup> Does the IP address identify a device on the internet, or a network of devices? Is the IP address an IPv4 or IPv6 address?<sup>140</sup>

- (b) **Cookies.** A different case would involve cookies that contain the user’s Google Account information (*e.g.*, cookies that contain a GAIA ID). I am also informed that a Google Account permits a user to either include a real name, or to supply a pseudonym. A Google Account can also include an email address. If Google associates the content of such cookies with a user’s Google Account, and if the account includes a person’s real name and email address, the content of those cookies is likely PI. However, I am informed that the cookies at issue in this case do *not* contain any GAIA IDs. The degree to which the cookies at issue in this case can reasonably be linked with a particular consumer will vary significantly, and turn on Google’s server-side practices and specific cookie attributes, including: Has Google employed measures that prevent data from being reasonably linked to an identified individual? Is the cookie a first or a third party cookie? For how long does the cookie persist on a user’s browser? Does the cookie contain a pseudonymous ID?

105. In sum, Mr. Hochman’s and Mr. Schneier’s assertion that the Data at Issue is PI or PII—regardless of the content of the specific data or the circumstances of how it is stored and processed—is generally inconsistent with American information privacy standards. None of the Data at Issue is associated with a user’s Google Account, which means the data is unauthenticated

---

<sup>139</sup> A dynamic IP address is one that changes frequently.

<sup>140</sup> See Psounis Rep. § III.G.1.a.



CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

(*i.e.*, not associated with a specific user’s identity), and Google implements policies and technical controls to prevent its re-identification.<sup>141</sup>

\*\*\*

106. The analyses and opinions in this report are based on the results of my research, my review and analysis of the materials provided to me, my education and training, and my experience on related topics. As additional materials and information become available or if the scope of discovery or the causes of action change in any material way, I reserve the right to amend, supplement, or update my analysis and conclusions.

*Paul M. Schwartz*  
Paul M. Schwartz  
June 7, 2022

---

<sup>141</sup> Psounis Rep. § III.A.; *See also* GOOG-CABR-00073880 at -882 (“Technical controls against inadvertent re-identification . . . include access control for any mapping between pseudonyms and other user identifiers (*e.g.*, mappings that may be used to append to pseudonymous data sets that contain stable identifiers), and anonymization techniques such as generalization of potentially unique data elements.”).

## APPENDICES

## A. Definitions of Personally Identifiable Information

<u>Source</u>	<u>Personally Identifiable Information</u>
Mr. Hochman's Expert Report	<p>“It is my opinion that an IP address, especially when combined with a user-agent string, constitutes personally identifiable information (‘PII’) because this data can be used to uniquely identify a user with a high probability of success. Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used to deanonymize previously anonymous data is considered PII[.]”<sup>142</sup></p> <p>“One metric for user identifiability is called entropy, measured in number of bits of data needed to uniquely identify a person. With a little less than 8 billion people on earth, 33 bits of data is needed to uniquely identify a person (<math>2^{33} = 8.6</math> billion). With around 330 million people in the United States, 29 bits of data is more than sufficient to identify a person (<math>2^{29} = 537</math> million).”<sup>143</sup></p>
Mr. Schneier's Expert Report	<p>“User data encompasses a range of information. Certain forms of personally identifying information—for example, name, address, Social Security number, passport or driver's license number, banking and credit card information—are often collected from users of products and services in the course of establishing accounts.”<sup>144</sup></p> <p>“Personally identifiable information is also generated in the course of using customer accounts. In the case of Internet services, these include highly personal records of users' online activity. Web browsing results in the accumulation of cookies and the creation of logs containing information from that web browsing. Full URLs often incorporate page titles, and therefore do more than just represent a web address; they may also indicate the content of the page.”<sup>145</sup></p>

<sup>142</sup> Hochman Rep. ¶ 105 (internal quotation marks omitted).

<sup>143</sup> *Id.* ¶ 231.

<sup>144</sup> Schneier ¶ 79.

<sup>145</sup> *Id.* ¶ 83.

FTC <sup>146</sup>	FTC staff recommends that the definition of PII only include information that is “reasonably” linkable to an individual.
Google’s Contracts and Policies <sup>147</sup>	<p>“Google interprets PII as information that could be used on its own to directly identify, contact, or precisely locate an individual. This includes:</p> <ul style="list-style-type: none"> <li>• email addresses</li> <li>• mailing addresses</li> <li>• phone numbers</li> <li>• precise locations (such as GPS coordinates - but see the note below)</li> <li>• full names or usernames</li> </ul> <p>For example, if you're a publisher whose contract prohibits you from passing PII to Google, the URLs of pages on your website that display ads by Google must not include email addresses, because those URLs would be passed to Google in any ad request. Google has long interpreted its PII prohibition in this way.</p> <p>Note: Certain product’s help centers and policies set out the limited means by which certain forms of PII may be sent to Google. For avoidance of doubt, this article does not amend such provisions. So, for example, certain products allow approximate location data to be sent to Google, provided the requirements of the applicable policies are met.</p> <p>Google interprets PII to exclude, for example:</p> <ul style="list-style-type: none"> <li>• pseudonymous cookie IDs</li> <li>• pseudonymous advertising IDs</li> <li>• IP addresses</li> <li>• other pseudonymous end user identifiers</li> </ul>

<sup>146</sup> Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, at 18-20 (March 26, 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

<sup>147</sup> Understanding PII in Google’s Contracts and Policies, Google Help Center, (2021), <https://support.google.com/analytics/answer/7686480>.

	<p>For instance, if an IP address is sent with an ad request (which will be the case with almost any ad request as a consequence of internet protocols), that transmission will not breach any prohibition on sending PII to Google.</p> <p>Note that data excluded from Google’s interpretation of PII may still be considered personal data or personal information under the GDPR, CCPA, and other privacy legislation. This article doesn't affect any contract provisions or policies relating to personal data or personal information under those laws.”</p>
U.S. Department of Labor - Guidance on the Protection of Personal Identifiable Information <sup>148</sup>	<p>“Personal Identifiable Information (PII) is defined as:</p> <p>Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (<i>e.g.</i>, name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, <i>i.e.</i>, indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.”</p>
Code of Federal Regulations - Part 200—Uniform Administrative Requirements, Cost Principles, and Audit	<p>“Personally Identifiable Information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become</p>

<sup>148</sup> U.S. Department of Labor, Guidance on the Protection of Personal Identifiable Information, (last visited Dec. 21, 2021), <https://www.dol.gov/general/ppii>.

Requirements for Federal Awards <sup>149</sup>	PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.”
NIST Computer Security Resource Center <sup>150</sup> - NIST SP 800-79-2 <sup>151</sup> under PII from EGovAct <sup>152</sup>	“Personally Identifiable Information; Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.”
NIST Computer Security Resource Center - NIST SP 800-37 Rev. 2 <sup>153</sup>	“Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.”
NIST Computer Security Resource Center - NISTIR 8053 <sup>154</sup> under PII from GAOReport 08-536, NIST SP 800-122 <sup>155</sup>	“Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”

<sup>149</sup> 2 C.F.R. § 200.1 (2021).

<sup>150</sup> National Institute of Standards and Technology, Glossary: Personally Identifiable Information (PII), (last visited Dec. 21, 2021), [https://csrc.nist.gov/glossary/term/personally\\_identifiable\\_information](https://csrc.nist.gov/glossary/term/personally_identifiable_information).

<sup>151</sup> Ferraiolo, et al., Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI) at 46, (July 2015), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-79-2.pdf>.

<sup>152</sup> E-GOVERNMENT ACT OF 2002, PL 107-347, December 17, 2002, 116 Stat 2899.

<sup>153</sup> See Ross, et al., Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy at 1, (December 2018), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf> (quoting Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016).

<sup>154</sup> Simson L. Garfinkel, De-Identification of Personal Information at 42-43, (October 2015), <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf>.

<sup>155</sup> GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, (May 2008), <http://www.gao.gov/new.items/d08536.pdf>.

U.S. General Services Administration <sup>156</sup>	“The term ‘PII,’ as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual.”
2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII) <sup>157</sup>	“PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified using information that is linked or linkable to said individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other information to identify a specific individual, could be used to identify an individual (e.g., Social Security Number (SSN), name, date of birth (DOB), home address, personal email).”
US Department of Energy - DOE O 203.2, Mobile Technology Management <sup>158</sup>	“Any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual’s identity, such as his/her name, Social Security number, date and place of birth, mother’s maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.”
US Department of Energy - DOE O 206.1 Chg1	“Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII can include

<sup>156</sup> U.S. General Services Administration, Rules and Policies - Protecting PII - Privacy Act, (Last Reviewed Jan. 12, 2020), <https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act>.

<sup>157</sup> Beth Anne Killoran, U.S. General Services Administration, 2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII), (Oct. 19, 2019), [https://www.gsa.gov/directive/gsa-rules-of-behavior-for-handling-personally-identifiable-information-\(pii\)-](https://www.gsa.gov/directive/gsa-rules-of-behavior-for-handling-personally-identifiable-information-(pii)-).

<sup>158</sup> Mobile Tech. Mgmt., US DOE 203.2 (May 15, 2014), <https://www.energy.gov/sites/default/files/2015/08/f25/o203.2.pdf>.

(MinChg), Department of Energy Privacy Program <sup>159</sup>	<p>unique individual identifiers or combinations of identifiers, such as an individual's name, Social Security number, date and place of birth, mother's maiden name, biometric data, etc.</p> <p>The sensitivity of PII increases when combinations of elements increase the ability to identify or target a specific individual. PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual is categorized as High Risk PII. Examples of High Risk PII include, Social Security Numbers (SSNs), biometric records (<i>e.g.</i>, fingerprints, DNA, etc.), health and medical information, financial information (<i>e.g.</i>, credit card numbers, credit reports, bank account numbers, etc.), and security information (<i>e.g.</i>, security clearance information).</p> <p>While all PII must be handled and protected appropriately, High Risk PII must be given greater protection and consideration following a breach because of the increased risk of harm to an individual if it is misused or compromised."</p>
US Department of Energy - DOE O 443.1C, Protection of Human Research Subjects <sup>160</sup>	<p>"Any information collected or maintained about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and any other personal information that is linked or linkable to a specific individual."</p>
Department of Commerce: Office of Privacy and Open Government - Safeguarding Information <sup>161</sup>	<p>"The term personally identifiable information refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.</p> <p>Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in harm, embarrassment, inconvenience, or unfairness to an individual. The following types of PII are considered</p>

<sup>159</sup> Minor Changes to Doe O 206.1, Dep't of Energy Priv. Program, US DOE 206.1 (Nov. 1, 2018), <https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder-chg1-minchg/@@images/file>.

<sup>160</sup> Prot. of Hum. Rsch. Subjects, US DOE 443.1C at 20 (Nov. 26, 2019). <https://www.directives.doe.gov/directives-documents/400-series/0443.1-BOrder-c/@@images/file> at 20.

<sup>161</sup> U.S. Dept. of Commerce, Safeguarding Information, (last updated Oct. 1, 2021), [https://www.osec.doc.gov/opog/privacy/pii\\_bii.html](https://www.osec.doc.gov/opog/privacy/pii_bii.html).

	<p>sensitive when associated with an individual: Social Security Number (including truncated form), place of birth, date of birth, mother's maiden name, biometric information, medical information (excluding brief references to absences from work), personal financial information, credit card or purchase card account numbers, passport numbers, potentially sensitive employment information (<i>e.g.</i>, performance ratings, disciplinary actions, and results of background investigations), criminal history, and any information that may stigmatize or adversely affect an individual.</p> <p>Context of information is important. The same types of information can be sensitive or non-sensitive depending upon the context. For example, a list of names and phone numbers for the Department's softball roster is very different from a list of names and phone numbers for individuals being treated for an infectious disease.</p> <p>If sensitive PII is electronically transmitted, it must be protected by secure methodologies, such as encryption, Public Key Infrastructure, or secure sockets layer. When in doubt, treat PII as sensitive."</p>
US Department of Education <sup>162</sup>	"Personally identifiable information (PII) includes information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information."
Family Educational Rights and Privacy Act Regulations, 34 CFR §99.3 <sup>163</sup>	<p>"The term includes, but is not limited to -</p> <ul style="list-style-type: none"> <li>(a) The student's name;</li> <li>(b) The name of the student's parent or other family members;</li> <li>(c) The address of the student or student's family;</li> <li>(d) A personal identifier, such as the student's social security number, student number, or biometric record;</li> <li>(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;</li> </ul>

<sup>162</sup> U.S. Dept. of Education, Protecting Student Privacy, (Last Visited Dec. 21, 2021), <https://studentprivacy.ed.gov/content/personally-identifiable-information-pii>.

<sup>163</sup> <https://www.ecfr.gov/current/title-34/subtitle-A/part-99>, (*citing* 20 U.S.C. 1232g, <https://www.govinfo.gov/content/pkg/USCODE-2019-title20/pdf/USCODE-2019-title20-chap31-subchapIII-part4-sec1232g.pdf>), (Last Visited Dec. 21, 2021).



	<p>(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or</p> <p>(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.”</p>
<p>California Business and Professions Code §22577(a) - Division 8. Special Business Regulations - Chapter 22. Internet Privacy Requirements <sup>164</sup></p>	<p>“(a) The term ‘personally identifiable information’ means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:</p> <ol style="list-style-type: none"> <li>(1) A first and last name.</li> <li>(2) A home or other physical address, including street name and name of a city or town.</li> <li>(3) An e-mail address.</li> <li>(4) A telephone number.</li> <li>(5) A social security number.</li> <li>(6) Any other identifier that permits the physical or online contacting of a specific individual.</li> <li>(7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.” </li></ol>
<p>Penal Code § 530.55, subdivisions (a) and (b) - Title 13. Of Crimes Against Property - Chapter 8. False Personation and Cheats <sup>165</sup></p>	<p>“(a) For purposes of this chapter, ‘person’ means a natural person, living or deceased, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity.</p> <p>(b) For purposes of this chapter, ‘personal identifying information’ means any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license, or identification number, social security number, place of employment, employee identification number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, United States Citizenship and Immigration Services-assigned number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the person, address or routing</p>

<sup>164</sup>California Business and Professions Code §22577(a) [https://leginfo.ca.gov/faces/codes\\_displaySection.xhtml?lawCode=BPC&sectionNum=22577](https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22577), (Last Visited Jun. 4, 2022).

<sup>165</sup> Cal. Penal Code § 530.55 (West 2007).

	code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number of an individual person, or an equivalent form of identification.”
CALJIC 15.61 <sup>166</sup>	<p>“The phrase, ‘personal identifying information’ means the [name, address, telephone number,] [health insurance [identification] number,] [taxpayer identification number,] [school identification number,] [state or federal driver's license number, or identification number,] [social security number,][place of employment,] [employee identification number,] [professional or occupational number][mother's maiden name,] [demand deposit number,] [savings account number,] [checking account number,] [PIN (personal identification number) or password,] [alien identification registration number,] [government passport number,] [date of birth,] [unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image,] [or] [other] [unique physical representation,] [unique electronic data including [information] identification number assigned to the person, address, or routing code,] [telephonic communication identifying information or access device,] [information contained in a birth or death certificate or credit card number of a person, or an equivalent form of identification].</p> <p>[For the purposes of this section, ‘person’ means a natural person, [living or deceased] firm, [association,] organization, partnership, business trust, company, corporation, limited liability company or public entity [, or any other legal entity].]”</p>
Song-Beverly Act <sup>167</sup>	<p>“(b) For purposes of this section ‘personal identification information,’ means information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number.”</p>
Video Privacy Protection Act of 1988 (VPPA) <sup>168</sup>	<p>“(a)(3) the term ‘personally identifiable information’ includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider...”</p> <p>“(d) Personally identifiable information.--Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.”</p>

<sup>166</sup> Cal. Jury Instr.--Crim. 15.61, Cal. Jury Instr.--Crim. 15.61.

<sup>167</sup> Song-Beverly Credit Card Act of 1971, Cal. Civ. Code § 1747.08 (West).

<sup>168</sup> 18 U.S.C.A. § 2710 (West).

Gramm-Leach-Bliley Act of 1999 (GLBA) <sup>169</sup>	<p>“(4) Nonpublic personal information</p> <p>(A) The term ‘nonpublic personal information’ means personally identifiable financial information--</p> <p>(i) provided by a consumer to a financial institution;</p> <p>(ii) resulting from any transaction with the consumer or any service performed for the consumer; or</p> <p>(iii) otherwise obtained by the financial institution.</p> <p>(B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title.</p> <p>(C) Notwithstanding subparagraph (B), such term--</p> <p>(i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but</p> <p>(ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.”</p>
Cable Communications Policy Act of 1984 <sup>170</sup>	<p>“(2) For purposes of this section, other than subsection (h)--</p> <p>(A) the term ‘personally identifiable information’ does not include any record of aggregate data which does not identify particular persons...”</p>
HIPAA Privacy Rule <sup>171</sup>	<p>“Protected Health Information. The Privacy Rule protects all ‘individually identifiable health information’ held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information ‘protected health information (PHI).’<sup>172</sup></p> <p>‘Individually identifiable health information’ is information, including demographic data, that relates to:</p> <p>the individual’s past, present or future physical or mental health or condition,</p> <p>the provision of health care to the individual, or</p> <p>the past, present, or future payment for the provision of health care to the individual,</p>

<sup>169</sup> 15 U.S.C.A. § 6809 (West).

<sup>170</sup> 47 U.S.C.A § 551(a)(2)(A).

<sup>171</sup> U.S. Dept. of Health and Human Services, Summary of the HIPAA Privacy Rule, (Last Reviewed Jul. 26, 2013), <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>.

<sup>172</sup> 45 C.F.R. § 160.103.

	<p>and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.<sup>173</sup> Individually identifiable health information includes many common identifiers (<i>e.g.</i>, name, address, birth date, Social Security Number).</p> <p>The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.</p> <p>De-Identified Health Information. There are no restrictions on the use or disclosure of de-identified health information.<sup>174</sup> De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.”</p>
--	--

---

<sup>173</sup> *Id.*

<sup>174</sup> 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

**B. Definitions of Personal Information**

<u>Source</u>	<u>Personal Information</u>
Google Privacy Policy <sup>175</sup>	“This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.” (emphasis added).
Cal. Civ. Code Sec. 1798.81.5(d)(1)	<p>“(1) ‘Personal information’ means either of the following:</p> <p>(A) An individual’s first name or first initial and the individual’s last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:</p> <ul style="list-style-type: none"> <li>(i) Social security number.</li> <li>(ii) Driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.</li> <li>(iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</li> <li>(iv) Medical information.</li> <li>(v) Health insurance information.</li> <li>(vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.</li> </ul> <p>(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.</p> <p>(2) “Medical information” means any individually identifiable information, in electronic or physical form, regarding the individual’s medical history or medical treatment or diagnosis by a health care professional.</p> <p>(3) “Health insurance information” means an individual’s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.</p>

<sup>175</sup> Google Privacy & Terms, Privacy Policy Key Terms (Last Accessed Jun. 3, 2022), <https://perma.cc/524M-5UH2>.

	(4) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."
Cal. Civ. Code § 1798.140(o)(1)	<p>"(o)(1) 'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:</p> <p>(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.</p> <p>(B) Any categories of personal information described in subdivision (e) of Section 1798.80.</p> <p>(C) Characteristics of protected classifications under California or federal law.</p> <p>(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.</p> <p>(E) Biometric information.</p> <p>(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.</p> <p>(G) Geolocation data.</p> <p>(H) Audio, electronic, visual, thermal, olfactory, or similar information.</p> <p>(I) Professional or employment-related information.</p> <p>(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).</p> <p>(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.</p> <p>(2) 'Personal information' does not include publicly available information. For purposes of this paragraph, 'publicly available' means information that is lawfully made available from federal, state, or local government records. 'Publicly available' does not mean biometric information collected by a business about a consumer without the consumer's knowledge.</p> <p>(3) 'Personal information' does not include consumer information that is de-identified or aggregate consumer information."</p>

California Civil Code §1798.3(a)	“The term ‘personal information’ means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.”
California Transactions Forms Business Transactions § 32:213. <sup>176</sup>	<p>“(6) ‘Personal information’ means any information that when it was disclosed identified, described, or was able to be associated with an individual and includes all of the following:</p> <ul style="list-style-type: none"> <li>(A) an individual's name and address;</li> <li>(B) electronic mail address;</li> <li>(C) age or date of birth;</li> <li>(D) names of children;</li> <li>(E) electronic mail or other addresses of children;</li> <li>(F) number of children;</li> <li>(G) the age or gender of children;</li> <li>(H) height;</li> <li>(I) weight;</li> <li>(J) race;</li> <li>(K) religion;</li> <li>(L) occupation;</li> <li>(M) telephone number;</li> <li>(N) education;</li> <li>(O) political party affiliation;</li> <li>(P) medical condition;</li> <li>(Q) drugs, therapies, or medical products or equipment used;</li> <li>(R) the kind of product the customer purchased, leased, or rented;</li> <li>(S) real property purchased, leased, or rented;</li> <li>(T) the kind of service provided;</li> <li>(U) Social Security number;</li> <li>(V) bank account number;</li> <li>(W) credit card number;</li> <li>(X) debit card number;</li> <li>(Y) bank or investment account, debit card, or credit card balance;</li> </ul>

<sup>176</sup> 5 Cal. Transactions Forms--Bus. Transactions § 32:213.

	(Z) payment history; and (AA) information pertaining to creditworthiness, assets, income, or liabilities. [Civ. Code, § 1798.83(e)(7)].”
California Practice Guide: Privacy Law <sup>177</sup>	“b. [6:813] ‘Personal information’ defined: The term “personal information” means any information that is maintained by the exchange that identifies or describes an individual, including, but not limited to, any of the following: — name; — social security number; — physical description; — home address; — home telephone number; — education; — financial matters; — medical or employment history; and — statements made by, or attributed to, the individual. [Gov.C. § 100503(a)(2)(C) (incorporating by reference definition of “personal information” contained in Civ.C. § 1798.3)]”
California Transactions Forms Business Transactions - § 32:211. Destruction of records of personal information <sup>178</sup>	“(5) ‘Personal information’ means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information. [Civ. Code, § 1798.80(e)].”
Regulations Under Specific Acts of Congress - Part 312. Children's Online Privacy Protection Rule <sup>179</sup>	“Personal information means individually identifiable information about an individual collected online, including: (1) A first and last name; (2) A home or other physical address including street name and name of a city or town; (3) Online contact information as defined in this section; (4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;

<sup>177</sup> H. Privacy of Information Maintained by California's Health Benefit Exchange, Cal. Prac. Guide Privacy Law Ch. 6-H.

<sup>178</sup> 5 Cal. Transactions Forms--Bus. Transactions § 32:211.

<sup>179</sup> 16 C.F.R. § 312.2 (2013).



	<p>(5) A telephone number;</p> <p>(6) A Social Security number;</p> <p>(7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;</p> <p>(8) A photograph, video, or audio file where such file contains a child's image or voice;</p> <p>(9) Geolocation information sufficient to identify street name and name of a city or town; or</p> <p>(10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.”</p>
Children’s Online Privacy Protection Act (COPPA) <sup>180</sup>	<p>“Personal information means individually identifiable information about an individual collected online, including:</p> <p>(1) A first and last name;</p> <p>(2) A home or other physical address including street name and name of a city or town;</p> <p>(3) Online contact information as defined in this section;</p> <p>(4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;</p> <p>(5) A telephone number;</p> <p>(6) A Social Security number;</p> <p>(7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;</p> <p>(8) A photograph, video, or audio file where such file contains a child's image or voice;</p> <p>(9) Geolocation information sufficient to identify street name and name of a city or town; or</p> <p>(10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.”</p>
§ 549. Definitions related to the Information Practice Act <sup>181</sup>	<p>“Under the provisions governing information practices, the term "personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone</p>

<sup>180</sup> 16 C.F.R. § 312.2.

<sup>181</sup> 13A Cal. Jur. 3d Consumer, etc. Protection Laws § 549.

	number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.”
--	---

### C. Definitions of Identifying Information

<u>Source</u>	<u>Identifying Information</u>
“Privacy-Preserving Data Sharing for Medical Research,” Stabilization, Safety, and Security of Distributed Systems: 23rd International Symposium <sup>182</sup>	“An identifier by itself is meaningless and is just a code. For example, any random combination of nine numbers very well may be a social security number, but without identifying information, there is no relevance, utility or vulnerability. Identifying information alone is not overly relevant, because it simply notes the existence of a person, without any detail of that person.”
FCRA	<p>“Notwithstanding the provisions of section 1681b of this title, a consumer reporting agency may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, or former places of employment, to a governmental agency.”<sup>183</sup></p> <p>“(b) Identifying information: Notwithstanding the provisions of section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information, signed by the Director or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an</p>

<sup>182</sup> Michael J. Fischer, Jonathon E. Hochman, and Daniel Boffa, “Privacy-Preserving Data Sharing for Medical Research,” Stabilization, Safety, and Security of Distributed Systems: 23rd International Symposium, SSS 2021, Virtual Event, [https://doi.org/10.1007/978-3-030-91081-5\\_6](https://doi.org/10.1007/978-3-030-91081-5_6) (Nov. 17–20, 2021) (“Hochman Paper”), at 2-3.

<sup>183</sup> 15 U.S.C.A. § 1681f.

	<p>investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.<sup>184</sup></p> <p>“(3) Procedures: The request of a victim under paragraph (1) shall--  (A) be in writing;  (B) be mailed to an address specified by the business entity, if any; and  (C) if asked by the business entity, include relevant information about any transaction alleged to be a result of identity theft to facilitate compliance with this section including--  (i) if known by the victim (or if readily obtainable by the victim), the date of the application or transaction; and  (ii) if known by the victim (or if readily obtainable by the victim), any other identifying information such as an account or transaction number.”<sup>185</sup></p> <p>“(3) Identity theft: The term “identity theft” means a fraud committed using the identifying information of another person, subject to such further definition as the Bureau may prescribe, by regulation.”<sup>186</sup></p>
18 U.S.C.A § 1029	<p>“(a)(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or...</p> <p>(e)(11) the term “telecommunication identifying information” means electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument.”</p>
10 CCR § 2593.2	<p>“A query shall allow for, but is not limited to, the following identifying information on an employer to inquire about the employer's coverage information on a specified date: Name of the employer; Name of the employer and a full or partial address of the employer, including, but not limited to, street name, city, and state; or FEIN.”</p>

<sup>184</sup> 15 U.S.C.A. § 1681u. (emphasis added).

<sup>185</sup> 15 U.S.C.A. § 1681g. (emphasis added).

<sup>186</sup> 15 U.S.C.A. § 1681a.

11 C.F.R. § 9410.2 11	<p>“Record means any item, collection, or grouping of information about an individual that is maintained by the Commission including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name or the identifying number, symbol, or other identifying information particularly assigned to the individual, such as finger or voice print or a photograph.</p> <p>Systems of records means a group of any records under the control of the Commission from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying information particularly assigned to the individual.”</p>
42 C.F.R. § 426.400	<p>(2) If the beneficiary has a representative, the representative-identifying information must include the following:</p> <ul style="list-style-type: none"> <li>(i) Name.</li> <li>(ii) Mailing address.</li> <li>(iii) Telephone number.</li> <li>(iv) E-mail address, if any</li> </ul>
5 C.F.R. § 581.203	<p>Sufficient identifying information must accompany the legal process in order to enable processing by the governmental entity named. Therefore, the following identifying information about the obligor, if known, is requested:</p> <ul style="list-style-type: none"> <li>(1) Full name;</li> <li>(2) Date of birth;</li> <li>(3) Employment number, social security number, Department of Veterans Affairs claim number, or civil service retirement claim number;</li> <li>(4) Component of the governmental entity for which the obligor works, and the official duty station or worksite; and</li> <li>(5) Status of the obligor, <i>e.g.</i>, employee, former employee, or annuitant.</li> </ul>
5 C.F.R. § 9301.13	<p>b) At a minimum, the request should contain sufficient identifying information to allow SIGAR to determine if there is a record pertaining to the individual making the request in a particular system of records. In instances when the requester's identification is insufficient to ensure disclosure to the individual to whom the information pertains in view of the sensitivity of the information, SIGAR reserves the right to solicit from the person requesting access to a record additional identifying information.</p>
34 U.S.C.A. § 12291	<p>(20) Personally <i>identifying information</i> or personal information</p>

	<p>The term “personally identifying information” or “personal information” means individually identifying information for or about an individual including information likely to disclose the location of a victim of domestic violence, dating violence, sexual assault, or stalking, regardless of whether the information is encoded, encrypted, hashed, or otherwise protected, including--</p> <p>(A) a first and last name;</p> <p>(B) a home or other physical address;</p> <p>(C) contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number);</p> <p>(D) a social security number, driver license number, passport number, or student identification number; and</p> <p>(E) any other information, including date of birth, racial or ethnic background, or religious affiliation, that would serve to identify any individual.</p>
22 U.S.C.A. § 2507a	<p>(1) Personally identifying information</p> <p>The term “personally identifying information” means individually identifying information for or about a volunteer who is a victim of sexual assault, including information likely to disclose the location of such victim, including the following:</p> <p>(A) A first and last name.</p> <p>(B) A home or other physical address.</p> <p>(C) Contact information (including a postal, email, or Internet protocol address, or telephone or facsimile number).</p> <p>(D) A social security number.</p> <p>(E) Any other information, including date of birth, racial or ethnic background, or religious affiliation, that, in combination with information described in subparagraphs (A) through (D), would serve to identify the victim.</p>
42 U.S.C.A. § 11360	<p>The term “personally identifying information” means individually identifying information for or about an individual, including information likely to disclose the location of a victim of domestic violence, dating violence, sexual assault, or stalking, including--</p> <p>(A) a first and last name;</p> <p>(B) a home or other physical address;</p> <p>(C) contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number);</p> <p>(D) a social security number; and</p>

	(E) any other information, including date of birth, racial or ethnic background, or religious affiliation, that, in combination with any other non-personally identifying information, would serve to identify any individual.
--	--

**D. Curriculum Vitae**

**PAUL M. SCHWARTZ**

Jefferson E. Peyser Professor of Law  
U.C. Berkeley School of Law  
Law School Building # 7200  
Berkeley, California 94720-7200  
website: [www.paulschwartz.net](http://www.paulschwartz.net)  
Email: [pschwartz@law.berkeley.edu](mailto:pschwartz@law.berkeley.edu)

Tel: 510-643-0352  
Fax: 510-643-2673

**EDUCATION:**

Yale Law School, J.D., June 1985  
Yale Law Journal, Volume 94, Senior Editor

Brown University, B.A. 1981, *magna cum laude*  
Honors in history and English, *Phi Beta Kappa*

**PUBLICATIONS**

**BOOKS:**

PRIVACY LAW FUNDAMENTALS (IAPP, 6th ed. 2022) (Daniel J. Solove, co-author)

PRINCIPLES OF THE LAW, DATA PRIVACY, AMERICAN LAW INSTITUTE (2020) (co-reporter with Daniel J. Solove)

INFORMATION PRIVACY LAW (ASPEN PUBLISHERS, 7th ed., 2020) (Daniel J. Solove, co-author)

INFORMATION PRIVACY STATUTES AND REGULATIONS, 2010-2011 (ASPEN PUBLISHERS, 2008) (Daniel J. Solove, co-editor)

ON-LINE SERVICES, DATA PROTECTION LAW AND PRIVACY: REGULATORY RESPONSES (Official Pub.of the European Union, Brussels, 1998)(Joel R. Reidenberg, co-author). Study carried out for the Commission of the European Communities (DGXV) regarding on-line privacy in Belgium, France, Germany, and the United Kingdom.

DATA PRIVACY LAW (Michie Publishing/Lexis Law Publishing, 1996), with Joel R. Reidenberg, co-author



**ARTICLES, ESSAYS,  
CHAPTERS:**

*Privacy and/or Trade*, 90 UNIVERSITY OF CHICAGO LAW REVIEW -- (forthcoming 2023), with Anupam Chander, co-author

*ALI Data Privacy Law: Overview and Black Letter Text*, 68 U.C.L.A. Law Review 1252 (2022), with Daniel Solove, co-author

*The Data Privacy Law of Brexit: Preference Formation, Transaction Costs, and Ideology*, 22 Theoretical Issues in Law 111 (2021)

*Global Data Privacy Law*, 94 N.Y.U. LAW REVIEW 771 (2019)

*Data Localization Under the CLOUD Act and the GDPR*, 2019 COMPUTER LAW REVIEW INTERNATIONAL 1, with Karl-Nikolaus Peifer, co-author

*Legal Access to the Global Cloud*, 118 COLUMBIA LAW REVIEW 1681 (2018)

*Transatlantic Data Privacy Law*, 106 GEORGETOWN LAW JOURNAL 115 (2017) with Karl-Nikolaus Peifer, co-author. Selected as 2017-2018 “Privacy Paper for Policymakers” by the Future of Privacy Forum.

*Systematic Government Access to Private-Sector Data in Germany*, in BULK COLLECTION 61 (Fred H. Cate & James X. Dempsey, eds. Oxford University Press, 2017)

*Foreword*, DETERMANN’S CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY (2017)

*Microsoft Ireland and a Level Playing Field for U.S. Cloud Companies*, 15 PVLR 1549 (Aug. 1, 2016), reprinted at 16 World Data Production Report 7 (July 28, 2016)

*The Value of Privacy Federalism*, in SOCIAL DIMENSIONS OF PRIVACY 324 (Beate Roessler & Dorota Mokorsinska, eds., Cambridge University Press, 2015)

*Reconciling Personal Information in the European Union and United States*, 102 CALIFORNIA LAW REVIEW 877 (2014), with Daniel J. Solove, co-author

*The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 HARVARD LAW REVIEW 1966 (2013)

*Privacy in the Cloud*, 161 UNIVERSITY PENNSYLVANIA LAW REVIEW 1623 (2013)

*Systematic Government Access to Private-Sector Data in Germany*,  
2 INTERNATIONAL DATA PRIVACY LAW 289 (2012)

*Reforming the concept of personally identified information: U.S. privacy law and PII 2.0* (with Daniel Solove), in NEUE REGULIERUNGSSCHUB IM DATENSCHUTZRECHT? 55 (Rolf H. Weber & Florent Thouvenin, eds.), Schulthess Verlag (Switzerland)(2012).

*PII 2.0: Privacy and a New Approach to Personal Information*, Privacy and Security Law Report, 11 PVLR 142 (January 10, 2012), with Daniel J. Solove, co-author

*The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. LAW REVIEW 1814 (2011), with Daniel Solove, co-author

*Regulating Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology*, 53 WILLIAM & MARY LAW REVIEW 351 (2011)

*Privacy, Ethics, and Analytics*, 9 IEEE SECURITY AND PRIVACY 66 (Nr. 3, May/June 2011)

*Data Protection Law and the Ethical Use of Analytics*, PRIVACY AND SECURITY LAW REPORT, 10 PVLR 70 (January 10, 2011)

*Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept*, 98 CALIFORNIA LAW REVIEW 1925 (2010), with Karl-Nikolaus Peifer, co-author

*Managing Global Data Privacy*, 10 PRIVACY ADVISOR 14 (Number 1, Jan.-Feb. 2010)

*Preemption and Privacy: Against a Federal Privacy Law*, 118 YALE LAW JOURNAL 902 (2009)

*Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes' Jorde Lecture*, 97 CALIFORNIA LAW REVIEW 407 (2009)

*From Victorian Secrets to Cyberspace Shaming, Review Essay*, 76 UNIVERSITY OF CHICAGO LAW REVIEW 1407 (2009)

*Keeping Track of Telecommunications Surveillance*, 52 COMMUNICATIONS OF THE ACM 24 (Sept. 2009)

*The Future of Tax Privacy*, 62 NATIONAL TAX JOURNAL 883 (2008)

*Reviving Telecommunications Surveillance Law*, 75 UNIVERSITY OF CHICAGO LAW REVIEW 287 (2008)

*Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 UNIVERSITY OF CHICAGO LAW REVIEW 261 (2008), with Ira S. Rubinstein and Ronald D. Lee, co-authors

*Anonymous Disclosure of Security Breaches*, with Edward J. Janger, co-author, in SECURING PRIVACY IN THE INTERNET AGE 221 (Anupam Chandler, Lauren Gelman & Margaret Jane Raden, eds., Stanford Law Books, 2008)

*Technological Change: Networked Intelligence and Information Privacy*, with Ronald D. Lee, co-author, in CIVIL LIBERTIES AND NATIONAL SECURITY: A HISTORICAL PERSPECTIVE 189 (Daniel Farber, ed., Russell Sage Foundation, 2008)

*Notification of Data Security Breaches*, 105 MICHIGAN LAW REVIEW 913 (2007), with Edward J. Janger, co-author

*Privacy Inalienability and Personal Data Chips*, in PRIVACY AND IDENTITY: THE PROMISE AND PERILS OF A TECHNOLOGICAL AGE (Katherine Strandburg & Daniela Stan Raicu, editors, Springer 2006)(abridged version of *Property, Privacy, and Personal Data*)

Review, *Beyond the War in Terrorism: Towards the New Information Network*, (Reviewing PHILIP HEYMANN, TERRORISM, FREEDOM, AND SECURITY: WINNING WITHOUT WAR (2003), with Ronald D. Lee, co-author, 103 MICHIGAN LAW REVIEW 1446 (2005)

*Privacy Inalienability and the Regulation of Spyware*, 20 BERKELEY TECHNOLOGY LAW JOURNAL 1269 (2005)

*Property, Privacy, and Personal Data*, 117 HARVARD LAW REVIEW 2055 (2004)

*Evaluating Telecommunications Surveillance in Germany: The Lessons of the Max Planck Institute Study*, 73 GEORGE WASHINGTON LAW REVIEW 1244 (2004)

*Lochner and Eldred: Copyright Term Extension and Intellectual Property as Constitutional Property*, with William M. Treanor, co-author, 112 YALE LAW JOURNAL 2331 (2003)

Review, *The New Privacy, Oversight of the Poor, and Total Information Awareness* (Reviewing JOHN GILLIOM, OVERSEERS OF THE POOR:

SURVEILLANCE, RESISTANCE AND THE LIMITS OF PRIVACY (2001)), with William Treanor, co-author, 101 MICHIGAN LAW REVIEW 2163 (2003)

*German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS LAW JOURNAL 751 (2003)

*Voting Technology and Democracy*, 77 NEW YORK UNIVERSITY LAW REVIEW 625 (2002)

*The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, with Edward J. Janger, co-author, 86 MINNESOTA LAW REVIEW 1219 (2002)

*Vote.com and Internet Politics: A Comment on Dick Morris's Version of Internet Democracy*, 34 LOYOLA L.A. LAW REVIEW 1071 (2001)

*Testimony*, Senate Committee on Commerce, Science and Transportation, Hearing on Internet Privacy, July 11, 2001

*Beyond Lessig's CODE for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WISCONSIN LAW REVIEW 743

Comment, *Free Speech versus Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STANFORD LAW REVIEW 1559 (2000)

*Internet Privacy and the State*, 32 CONNECTICUT LAW REVIEW 815 (2000). Lead article in symposium issue of the CONNECTICUT LAW REVIEW; the issue also contains five responses to my article.

*Charting a Privacy Research Agenda: Responses, Agreements, and Reflections*, 32 CONNECTICUT LAW REVIEW 929 (2000). Responding to the five scholars who commented on my article, *Internet Privacy and the State*.

*Democracy and Privacy in Cyberspace*, 52 VANDERBILT LAW REVIEW 1609 (1999)

*Privacy and the Economics of Personal Health Care Information*, 76 TEXAS LAW REVIEW 1 (1997)

*European Data Protection Law and Medical Privacy*, in GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 392 (Mark A. Rothstein, ed., Yale University Press, 1997)

*Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA LAW REVIEW 533 (1995)

*European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA LAW REVIEW 471 (1995)

*The Protection of Privacy in Health Care Reform*, 48 VANDERBILT LAW REVIEW 295 (1995)

*Constitutional Change and Constitutional Legitimation: The Example of German Unification*, 31 HOUSTON LAW REVIEW 1027 (1994)

*Testimony to Government Information, Justice, Transportation, and Agriculture Subcommittee of House Committee on Government Operations, House of Representatives, 103<sup>rd</sup> Congress, reprinted in FAIR HEALTH INFORMATION PRACTICES ACT OF 1994 (2d Session on H.R. 4077) 358 (1994)*

*Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS LAW JOURNAL 1321 (1992)

Book Review, *The Oversight of Data Protection*, 39 AMERICAN JOURNAL OF COMPARATIVE LAW 618 (1991)

Review Essay, *Baby M. in West Germany*, 89 COLUMBIA LAW REVIEW 347 (1989)

*The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AMERICAN JOURNAL OF COMPARATIVE LAW 675 (1989)

Note, *Parental Rights and the Habilitation Decision for Mentally Retarded Children*, 94 YALE LAW JOURNAL 1715 (1985)

#### **SHORTER WORKS- COLUMNS & OP-EDS:**

*Foreward*, Determann's California Privacy Law: Practical Guide and Commentary (4th ed., 2020)

*Preface: Privacy Law in the Pandemic Year*  
*Korean Legislation Research Institute, Issue Brief: Data Protection (October 2020)*

*Illusions of consent and COVID-19 tracking apps*  
IAPP Privacy Perspectives (May 19, 2020)

*Protecting privacy on COVID-19 surveillance apps*  
IAPP Privacy Perspectives (May 8, 2020)

*Microsoft Ireland and a Level Playing Field for U.S. Cloud Companies*  
15 PVLR 1549 (Aug. 1, 2016), reprinted at 16 World Data  
Production Report 7 (July 28, 2016)  
*The Delayed Revolution in Digital Financial Services*, TechCrunch.com  
(April 9, 2016)

*Risk and High Risk: Walking the GDPR Tightrope*, IAPP Privacy  
Perspectives (March 29, 2016)

*Navigating the cloud: key regulatory issues to know*, DAILY JOURNAL, ASIA  
SUPPLEMENT (Oct. 22, 2014), with Behnam Dayanim

*Defining “Personal Data” in the European Union and United States*, 13  
PVLR 1581 (Sept. 15 2014) with Daniel J. Solove, co-author,  
reprinted at 14 WORLD DATA PROTECTION REPORT 4 (Sept. 2014)

*Differing Privacy Regimes: A Mini-Poll on Mutual EU-U.S. Distrust*, IAPP  
PRIVACY PERSPECTIVES (July 22, 2014)

*The Battle for Leadership in Education Privacy Law*, SAFEgov.org (Mar.  
27, 2014) with Daniel Solove

*In Practice: The ‘California Effect’ on Privacy Law*, THE RECORDER, Jan. 2,  
2014

*Testimony, Balancing Privacy and Opportunity in the Internet Age*, California  
Assembly Informational Hearing, Dec. 12, 2013

*Blog, What Is Personally Identifiable Information (PII)? Finding Common  
Ground in the EU and US*, CONCURRING OPINIONS (June 26, 2013)  
with Daniel Solove

*EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed  
Regulation*, 12 PVLR 718 (Apr. 28, 2013)

*Privacy Firsts at Berkeley Law*, SAN FRANCISCO CHRONICLE E5 (Feb.  
25, 2012)  
Blog, *PII 2.0*, TECHNOLOGY | POLICY | ACADEMICS (Jan. 16, 2012)  
with Daniel Solove

Blog, *Google Ngram and Information Privacy*, GOOGLE POLICY BY THE  
NUMBERS (Jan. 9, 2012)(Daniel J. Solove, co-author)

*Amend telecommunications surveillance laws*, SAN FRANCISCO CHRONICLE  
H6 (March 1, 2009)

Essay, *Bye to chads; hello to what?*, NATIONAL LAW JOURNAL A24 (June

11, 2001)

*Book Review, The Lawyer's Bookshelf: You Say You Want a Revolution*, By Reed E. Hundt (2000), NEW YORK LAW JOURNAL 2 (July 10, 2000)

*Book Review, The Lawyer's Bookshelf: The Code Book*, By Simon Singh (1999), NEW YORK LAW JOURNAL 2 (Dec. 21, 1999)

*American Data Protection Law Today*, RECUEIL DES COMMUNICATIONS/ COLLECTION OF PAPERS, Twelfth Annual Conference of Data Protection Commissioners (France, 1990), *reprinted in* TRANSNATIONAL DATA REPORT 20 (Netherlands 1990); Privacy Laws & Business 11 (October 1990) (England); and XII Conférence Internationale des Commissaires à la Protection des Données (France, 1990) (French translation)

*Recent Public Trends in West Germany*, PARTISAN REVIEW 235 (1987). Analysis of a debate among German historians about the contemporary meaning of the Holocaust.

#### GERMAN LANGUAGE PUBLICATIONS:

*Datentreuhändermodelle – Sicherheit vor Herausgabeverlangen US-amerikanischer Behörden und Gerichte?*, COMPUTER UND RECHT 165 (3/2017) (“Data Fiduciary Model – Protection from Data Requests of U.S. Governmental Authorities and Courts?”) with Karl-Nikolaus Peifer

*Zur Architektur des Datenschutzes in den U.S.A.*, in DATENSCHUTZ IM DIGITALEN ZEITALTER – GLOBAL, EUROPÄISCH, NATIONAL (2015) (“The Architecture of Data Protection in the USA,” in Data Protection in the Digital Age: Global, European, National)

*Referat*, in Verhandlung des 69. Deutschen Juristentages: München 2012, Band II/1, O73 (2013) (Presentation, in Proceedings of the 69th German Jurists’ Forum)

*“Personenbezogene Daten” aus internationaler Perspektive*, (An International Perspective on “Personal Data”), ZEITSCHRIFT FÜR DATENSCHUTZ 97 (March 20, 2011)

*Kehrtwende beim Datenschutz* (Turning Point for Data Protection Law)(translation Al Sopot), BERLIN TAGESSPIEGEL, Sept. 5, 2002 (op-ed about privacy developments after 9/11)

*Das Übersetzen im Datenschutz: Unterschiede zwischen deutschen und amerikanischen Konzepten der "Privatheit"* (Translating the Legal Concept



of "Privacy": Differences between American and German Approaches), 8 RECHT DER DATENVERARBEITUNG 8 (1992), *reprinted in* ÜBERSETZEN, VERSTEHEN, BRÜCKEN BAUEN (Erich Schmidt Press, Berlin, 1993)

*Die neuesten Entwicklungen im amerikanischen Datenschutzrecht* (New Trends in American Data Protection Law), 5 RECHT DER DATENVERARBEITUNG 153 (1989)

**EXPERT WITNESS  
& CONSULTING:**

Expert cases include *Gerling Global Reinsurance Corp v. Quackenbush*, 2000 WL 777978 (E.D. Cal. 2002), *reversed* *American Ins. Ass'n v. Garamendi*, 539 U.S. 396 (2003). Worked on this case as part of an international team of lawyers assisting the State of California in defense of the Holocaust Insurance Relief Act (HIVRA). State statute required insurance companies to disclose to the State of California any involvement with insurance policies of Holocaust victims. Provided affidavits and advice to California regarding German information privacy law and whether it prohibited compliance with HIVRA.

Other reported opinions on cases on which I worked as expert include: *In re: Vitamins Antitrust Litigation*, 2001 WL 1049433 (D.D.C. 2001); and *VWAG v. Monceaux*, 909 S.W. 2d 900 (Texas 1995).

Past clients include the Commission of the European Union, the State of California, Volkswagen AG, and other multinational corporations.

**GRANTS  
AND AWARDS:**

American Academy in Berlin, Berlin Prize Fellow, Germany, Fall 2002; German Marshall Fund, Transatlantic Fellow, Transatlantic Center, Brussels, Belgium, Spring 2003; Funded Research Project: *Post 9-11 Developments in Telecommunications Privacy Law in the U.S., Germany, and the European Union*

Other Grants and Awards: Thyssen Foundation, 2012 (with University of Cologne Law School); German Academic Exchange Award, 1997; Harry Frank Guggenheim Foundation Fellowship, Spring 1995; Fulbright Scholarship, 1991; Alexander von Humboldt Scholar, 1986-1988.

**ADVISORY BOARDS:**



Brussels Privacy Hub, Vrije University Brussels, Belgium, Advisory Board Member

INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY, Oxford University Press, Editorial Board Member

INTERNATIONAL DATA PRIVACY LAW, Oxford University Press, Editorial Board Member

ZEITSCHRIFT FÜR DATENSCHUTZ (Data Protection Journal), Editorial Board Member

Future of Privacy Forum, Washington D.C., Board of Advisors

Trusted Computing Academic Advisory Board, (TCAAB), Microsoft Corporation, Redmond, Washington (Member, 2003-2011). The TWCAAB advised Microsoft on its trusted computing initiative and other policy and computing issues.

**PROFESSORSHIPS  
AND ACADEMIC  
POSITIONS:**

Co-Reporter, Data Privacy Principles Project, American Law Institute, 2013 to 2020. Project approved May 2019 by ALI, finalized and published December 2020

Jefferson E. Peyser Professor of Law, University of California-Berkeley School of Law, Boalt Hall, 2014 to present

Professor of Law, University of California-Berkeley School of Law, Boalt Hall, 2006-2014

Anita and Stuart Subotnick Professor of Law, Brooklyn Law School, 2004-2006; Professor of Law, Brooklyn Law School, 1998-2004.

Professor of Law, University of Arkansas School of Law (Fayetteville), Fall 1995- Spring 1998. Associate Professor, 1992-1995, Assistant Professor, 1988- 1992.

Guest Scholar, Institute for Labor, Economic and Civil Law, Goethe University, Frankfurt/Main, Germany, Summer 1998, Summer 1997, Summer 1996, Summer 1995, Summer 1993, Summer 1992, Summer 1991, Summer 1990, Summer 1989.

Guest Professor, University of Nantes, School of Law & Political Science, Nantes, France, Summer 1993, Summer 1992.

**MEMBERSHIP, PROFESSIONAL  
SOCIETIES:**

American Law Institute, Elected 2005  
New York Bar, Admitted September 2014  
Arkansas Bar, Admitted February 1988

German Academic Exchange Alumni Association  
Alexander von Humboldt Foundation Alumni Association  
Phi Beta Kappa, Brown University, 1981

### **E. Court Testimony in the Last Four Years**

- Expert Legal Opinion of Professor Paul M. Schwartz in the case entitled *Barak v. Facebook Ireland Limited*, Case No. 32672-02-17, pending in the District Court in Tel Aviv, Israel, March 14, 2019.
- Expert Opinion of Professor Paul M. Schwartz in the case entitled *Calhoun v. Google*, Case No. 4:20-cv-05146-YGR-SVK, pending in the Northern District of California, January 22, 2022.

### **F. Materials Considered**

#### Filed Documents:

- Third Amended Complaint (Dkt. 395-2)
- Declaration. of Alexei Svitkine (Dkt. 112-5)
- Report of Dr. Zubair Shafiq, *Calhoun v. Google*, 5:20-cv-05146-LHK, (Dkt. 340-19)
- Declaration of David Monsees, *Calhoun v. Google*, 5:20-cv-05146-LHK, (Dkt. No. 428-22)

#### Public Documents:

- J. Hochman, M. Fischer and D. Boffa Privacy-Preserving Data Sharing for Medical Research, Yale University (2021)
- Michael J. Fischer, Jonathon E. Hochman, and Daniel Boffa, “Privacy-Preserving Data Sharing for Medical Research,” Stabilization, Safety, and Security of Distributed Systems: 23rd International Symposium, SSS 2021, Virtual Event, [https://doi.org/10.1007/978-3-030-91081-5\\_6](https://doi.org/10.1007/978-3-030-91081-5_6) (Nov. 17–20, 2021)
- Paul M. Schwartz & Daniel J. Solove, Reconciling Personal Information in the United States and European Union (2014)
- Paul M. Schwartz & Daniel J. Solove, Defining “Personal Data” in the European Union and U.S. (2014)
- Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information (2011)
- Paul M. Schwartz, “Personenbezogene Daten” aus internationaler Perspektive, Zeitschrift für Datenschutz 97 (3/2011) (“Personal-specific Data” from an International Perspective)
- Federal Trade Commission (F.T.C.) Report, “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers” (March 26, 2012)
- In the Matter of Protecting the Privacy of Customers of Broadband & Other Telecommunications Services, WC Docket No. 16-106, Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission (May 27, 2016), <https://perma.cc/2EJZ-ENW8>
- Christina H. Kroll, CCPA: The California Senate is Not Ready to Expand the Consumer Right of Action Proskauer Priv. L. Blog (May 17, 2019), <https://perma.cc/699Z-QENL>
- Platforms Program Policies, Google Help Center, (Last Updated Apr. 1, 2022), <https://perma.cc/7D86-XR54>

- Best Practices to Avoid Sending Personally Identifiable Information (PII), Analytics Help Center, (2021), <https://perma.cc/L7LG-CG7W>
- Prabhakar Raghavan, Raising the Bar on Transparency, Choice and Control in Digital Advertising, (May 7, 2019), Google Ads & Commerce Blog, <https://perma.cc/HQH3-PPBE>
- The Privacy Sandbox, Chromium Blog, <https://perma.cc/7GGQ-7YV7> (last accessed Jun. 4, 2022)
- Justin Schuh, Building a more private web: A path towards making third party cookies obsolete, Chromium Blog, (Jan. 14, 2020), <https://perma.cc/8LCF-7N4A>
- Policy Against Fingerprints and Locally Shared Objects, Google Analytics Help Center, <https://perma.cc/V44X-GEZK> (2022)
- Interoperability guidance for vendors working with Google via the IAB TCFv2.0, Google Ad Manager Help Center, <https://perma.cc/EC8S-MVJK> (2022)
- Requirements for third-party ad serving, Google Advertising Policies Help, <https://perma.cc/JP2W-8H7Z> (2022)
- Federal Trade Commission (F.T.C.), Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 26, 2012)
- Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, at 18-20 (March 26, 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>
- Understanding PII in Google's Contracts and Policies, Google Help Center, (2021), <https://support.google.com/analytics/answer/7686480>
- U.S. Department of Labor, Guidance on the Protection of Personal Identifiable Information, (last visited Dec. 21, 2021), <https://www.dol.gov/general/ppii>
- National Institute of Standards and Technology, Glossary: Personally Identifiable Information (PII), (last visited Dec. 21, 2021), [https://csrc.nist.gov/glossary/term/personally\\_identifiable\\_information](https://csrc.nist.gov/glossary/term/personally_identifiable_information)
- Ferraiolo, et al., Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI) at 46, (July 2015), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-79-2.pdf>
- Ross, et al., Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy at 1, (December 2018), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>
- Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016
- Simson L. Garfinkel, De-Identification of Personal Information at 42-43, (October 2015), <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf>
- GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, (May 2008), <http://www.gao.gov/new.items/d08536.pdf>
- U.S. General Services Administration, Rules and Policies - Protecting PII - Privacy Act, (Last Reviewed Jan. 12, 2020), <https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act>
- Beth Anne Killoran, U.S. General Services Administration, 2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII), (Oct. 19, 2019),

[https://www.gsa.gov/directive/gsa-rules-of-behavior-for-handling-personally-identifiable-information-\(pii\)-](https://www.gsa.gov/directive/gsa-rules-of-behavior-for-handling-personally-identifiable-information-(pii)-)

- Mobile Tech. Mgmt., US DOE 203.2 (May 15, 2014), <https://www.energy.gov/sites/default/files/2015/08/f25/o203.2.pdf>
- Minor Changes to Doe O 206.1, Dep't of Energy Priv. Program, US DOE 206.1 (Nov. 1, 2018), <https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder-chg1-minchg/@@images/file>
- Prot. of Hum. Rsch. Subjects, US DOE 443.1C at 20 (Nov. 26, 2019), <https://www.directives.doe.gov/directives-documents/400-series/0443.1-BOrder-c/@@images/file> at 20
- U.S. Dept. of Commerce, Safeguarding Information, (last updated Oct. 1, 2021), [https://www.osec.doc.gov/opog/privacy/pii\\_bii.html](https://www.osec.doc.gov/opog/privacy/pii_bii.html).
- U.S. Dept. of Education, Protecting Student Privacy, (Last Visited Dec. 21, 2021), <https://studentprivacy.ed.gov/content/personally-identifiable-information-pii>.
- Family Educational Rights and Privacy Act Regulations, 34 CFR §99.3 <https://www.ecfr.gov/current/title-34/subtitle-A/part-99>,
- 20 U.S.C. 1232g, <https://www.govinfo.gov/content/pkg/USCODE-2019-title20/pdf/USCODE-2019-title20-chap31-subchapIII-part4-sec1232g.pdf>), (Last Visited Dec. 21, 2021)
- California Business and Professions Code §22577(a) [https://leginfo.ca.gov/faces/codes\\_displaySection.xhtml?lawCode=BPC&sectionNum=22577](https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22577), (Last Visited Jun. 4, 2022)
- Google Privacy & Terms, Privacy Policy Key Terms (Last Accessed Jun. 3, 2022), <https://perma.cc/524M-5UH2>
- U.S. Dept. of Health and Human Services, Summary of the HIPAA Privacy Rule, (Last Reviewed Jul. 26, 2013), <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>
- App. C (42 C.F.R. § 426.400, 5 C.F.R. § 581.203, 34 U.S.C.A. § 12291, 22 U.S.C.A. § 2507a, 42 U.S.C.A. § 11360)
- General Data Protection Regulation, Article 4 (European Union)
- ALI Data Privacy Principles
- CCPA § 1798.140(v)(1)
- CCPA § 1798.81.5(d)(1)
- CCPA § 1798.140(o)(1)
- CCPA § 1798.81.5(d)(1)
- Cal. Civ. Code § 1798.140(o)
- Cal. Civ. Code § 1798.155(b)
- California Consumer Privacy Act of 2018: Consumer Remedies, CA Sen. Bill. 561 (2019)
- Cal. Civ. Code § 1798.150(a)(1)
- Cal. Civ. Code § 1798.81.5(d)(1)
- Cal. Civ. Code § 1798.140(o)(1)
- Cal. Civ. Code § 1798.145(a)
- Cal. Civ. Code, §1798.140(o)(3)
- Cal. Civ. Code § 1798.140(r)
- Cal. Civ. Code § 1798.145(p)

- Cal. Civ. Code § 1798.145(j)
- 2 CFR § 200.79, <https://perma.cc/P9HC-XF2U>
- 2 CFR § 200.338, <https://perma.cc/8E4S-2XMY>
- 2 CFR § 200.1
- 2 C.F.R. § 200.1 (2021)
- E-GOVERNMENT ACT OF 2002, PL 107-347, December 17, 2002
- Cal. Penal Code § 530.55 (West 2007)
- Cal. Jury Instr.--Crim. 15.61, Cal. Jury Instr.--Crim. 15.61
- Song-Beverly Credit Card Act of 1971, Cal. Civ. Code § 1747.08 (West)
- 18 U.S.C.A. § 2710 (West)
- 15 U.S.C.A. § 6809 (West)
- 47 U.S.C.A § 551(a)(2)(A)
- 45 C.F.R. § 160.103
- 20 U.S.C. §1232g
- 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b)
- Cal. Civ. Code Sec. 1798.81.5(d)(1)
- Cal. Civ. Code § 1798.140(o)(1)
- 20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99
- California Civil Code §1798.3(a)
- 5 Cal. Transactions Forms--Bus. Transactions § 32:213
- Gov.C. § 100503(a)(2)(C)
- Civ.C. § 1798.3
- H. Privacy of Information Maintained by California's Health Benefit Exchange, Cal. Prac. Guide Privacy Law Ch. 6-H
- 5 Cal. Transactions Forms--Bus. Transactions § 32:211
- 16 C.F.R. § 312.2 (2013)
- 13A Cal. Jur. 3d Consumer, etc. Protection Laws § 549
- 15 U.S.C.A. § 1681f
- 18 U.S.C.A § 1029
- 10 CCR § 2593.2
- 11 C.F.R. § 9410.2
- 15 U.S.C.A. § 1681u
- 15 U.S.C.A. § 1681g
- 15 U.S.C.A. § 1681a
- 42 C.F.R. § 426.400
- 5 C.F.R. § 581.203
- 5 C.F.R. § 9301.13
- 34 U.S.C.A. § 12291
- 22 U.S.C.A. § 2507a
- 42 U.S.C.A. § 11360

#### Expert Reports:

- Hochman Report
- Schneier Report
- Psounis Rebuttal Report
- Zervas Rebuttal Report

Produced Documents:

- GOOG-CALH-00027147
- GOOG-CABR-04400013
- GOOG-CALH-00027147
- GOOG-BRWN-00029004
- GOOG-BRWN-00029004
- GOOG-CABR-00073880